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)	P2019-ND-021 (File #008523)
Date notice received by OIPC	April 27, 2018
Date Organization last provided information	November 28, 2018
Date of decision	February 14, 2019
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 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 all or some of the following information: • first and last name, • email address, • telephone number, • physical address, • social insurance number, • date of birth, • employment status, • housing status, • marital status, • salary, • total debt, • vehicle value, and • loan amount requested. This information is about an identifiable individual and is "personal information" as defined in section 1(1)(k) of PIPA.

❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• On April 2, 2018, an employee of the Organization received an online loan application for a potential new member. • The employee forwarded the email containing the application to the Branch Manager for review and action. However, Microsoft Outlook auto-populated the name of the last person the employee emailed who was not authorized to receive the information and was outside of the Organization's network. • The employee discovered the incident the same day, immediately after sending the email. • The information was disclosed to one individual who is an existing and current member of the Organization.
Affected individuals	The incident affected one individual residing in Alberta
Steps taken to reduce risk of harm to individuals	• Made multiple attempts to contact the unauthorized individuals but was told he was not available to contact. • Will disable the auto-complete setting for all new employees as well as agents moving to different workstations.
Steps taken to notify individuals of the incident	The affected individual was notified by telephone on April 3, 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 that "The information disclosed could cause financial loss to the Individual" and also "The information disclosed is sensitive and provides the opportunity for identity theft". In my view, the contact, identity and financial information at issue could be used to cause the significant harms of identity theft, fraud and financial loss. The contact information, as well as email address, could be used for unsolicited telephone calls, emails and phishing. I have previously found phishing to be a significant harm.
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 that "The information is highly sensitive and was identified immediately" and "The information was disclosed to one individual who is an existing and current member of [the Organization]". Further, "Multiple attempts have been made to contact the unauthorized Individual and we have been told that he is in the hospital after suffering a head injury. We also attempted to recall the email and were not successful".

	In my view, there is a real risk of significant harm. Although the incident resulted from human error and not malicious intent, the Organization has reported that the unintended recipient, who is known to the Organization, is unable to confirm that the information was received or securely destroyed and thus remains exposed.

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.

The contact, identity and financial information at issue could be used to cause the significant harms of identity theft, fraud and financial loss. The contact information, as well as email address, could be used for unsolicited telephone calls, emails and phishing. I have previously found phishing to be a significant harm. Although the incident resulted from human error and not malicious intent, the Organization has reported that the unintended recipient, who is known to the Organization, is unable to confirm that the information was received or securely destroyed and thus remains exposed.

I require the Organization to notify the affected individual in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified the affected individual by telephone on April 3, 2018 in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner