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)	P2020-ND-174 (File #17348)
Date notice received by OIPC	May 8, 2020
Date Organization last provided information	May 8, 2020
Date of decision	December 3, 2020
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: • name, • date of birth, • address, • email address, • social insurance number, • marital status, • telephone number (residential and work), • occupation, • employer, • total assets and liabilities, • net worth, • income, and • salary information. This information is about an identifiable individual 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 4, 2020, an employee was conversing with 2 separate individuals on 2 separate loan applications. • An email was subsequently sent to one of the individuals with an attachment containing a completed statement of affairs for another individual. • The incident was discovered the same day when the email recipient reported the error to the Organization.
Affected individuals	The incident affected 1 resident of Alberta.
Steps taken to reduce risk of harm to individuals	Coaching employees to take a second look at an attachment prior to hitting the send button on an email.
Steps taken to notify individuals of the incident	The affected individual was notified by telephone on May 5, 2020 and May 7, 2020.
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 described the possible harm that might result from this incident as "Risk of harm is identity theft to the individual and reputational risk to the credit union ". I agree with the Organization's assessment. A reasonable person would consider the contact, identity, employment and financial information at issue could be used to cause the harms of identity theft and fraud. Email address could be used for phishing purposes, increasing vulnerability to 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 that "Likelihood [of harm] is low as 1 individual information is exposed and the single individual who received the information notifed [sic] the credit union immediately." In my view, the likelihood of harm resulting from this incident is decreased because the breach resulted from human error and not malicious intent, and because the unintended recipient of the email reported the error to the Organization. However, the Organization did not report any efforts to recall the email or confirm the unintended recipient deleted the email and did not disclose it further.

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, identity, employment and financial information at issue could be used to cause the harms of identity theft and fraud. Email address could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms. The likelihood of harm resulting from this incident is decreased because the breach resulted from human error and not malicious intent, and because the unintended recipient of the email reported the error to the Organization. However, the Organization did not report any efforts to recall the email or confirm the unintended recipient deleted the email and did not disclose it further. I require the Organization to notify the affected individual 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 May 5, 2020 and on May 7, 2020. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner