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	TransCanada Credit Union Ltd. (Organization)
Decision number (file number)	P2016-ND-08 (File #000509)
Date notice received by OIPC	March 24, 2015
Date Organization last provided information	March 26, 2015
Date of decision	February 11, 2016
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 incorporated in Alberta and is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, • email address, • banking provider, • details of a requested financial transaction. 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 February 27, 2015, the personal information of one of the Organization's members was inadvertently emailed to 1126 other members (all employees of the Organization). • Several of the unauthorized recipients responded to the email by informing the Organization of the error.
Affected individuals	One individual was affected.
Steps taken to reduce risk of harm to individuals	• Emails sent from the Organization's email server include a disclaimer that advises against unauthorized use or disclosure of email information received in error. • A recall was sent to recipients of the email upon discovery of the incident. Unread emails were recalled. • An email response about the incident was sent to individuals who had acknowledged reading the email. • The Organization reported that steps will be taken to develop and offer organization-wide mandatory privacy and email training and to review personal information protection controls.
Steps taken to notify individuals of the incident	The affected individual was notified via telephone.
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 type of harm that could result from the incident is fraud/identity theft. However, the Organization also reported that "It is unlikely that an individual armed with the information inadvertently disclosed would be able to facilitate fraud, without other pertinent information." I agree with the Organization that the information at issue, in itself, could be used to cause the harms of fraud and identity theft. I also note that the unintended recipients of the email were all employees of the Organization; their proximity to the affected individual could be exploited to obtain additional information to facilitate fraud. In addition, the email address could be used to cause the harm of phishing. 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 assessed the likelihood of harm resulting from this incident to be low "Due to the minimal amount of personal information that was revealed." In my view, the likelihood of harm resulting from this incident is increased because the personal information was disclosed to 1126 unauthorized individuals and not all copies of the email communication were recalled.

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 personal information at issue, by itself, could be used to cause the harms of fraud and identity theft. Further, the unintended recipients of the email were all employees of the Organization and their proximity to the affected individual could be exploited to obtain additional information to facilitate fraud. The email address could also be used to cause the harm of phishing. These are significant harms. In my view, the likelihood of harm resulting from this incident is increased because the personal information was disclosed to 1126 unauthorized individuals and not all copies of the email communication were recalled.

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 in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner