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)	P2019-ND-137 (File #012632)
Date notice received by OIPC	March 26, 2019
Date Organization last provided information	March 26, 2019
Date of decision	August 14, 2019
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify those individuals 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 an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The Organization reported that the incident involved the following information: • name, • home address, • salary information, • account number, • account information (including, among other things, social insurance number, driver's license number and expiry date, credit history, and application forms and approvals for lending facilities, such as lines of credit.). 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	• A former employee, without authorization, electronically transferred funds from lines of credit, loans and/or members' savings accounts to external bank accounts controlled by the employee and/or the employee's family members. • In addition to unauthorized access and use of personal information on the Organization's information technology systems, four physical files relating to four individual members affected by the scheme cannot be located and are suspected to have been taken or destroyed by the employee. • The breach was discovered on January 7, 2019, when a member contacted the Organization and inquired about a line of credit opened on her account without her knowledge. • The Organization found that the line of credit was opened by the employee on March 9, 2018, and funds were drawn and deposited to an external account. Documentation for these transactions was missing. • The incidents took place between March 10, 2011 and January 3, 2019.
Affected individuals	The incident affected 21 individuals.
Steps taken to reduce risk of harm to individuals	• Terminated the employee and removed access to premises and all systems. • Engaged legal counsel, third-party forensic investigators and accountants. • Reported breach to data protection financial regulators. • Switched banking platforms, will remediate any gaps in security systems and engage in a full review and update of procedures and policies. • Continuing to investigate to assess the scope of the incident. • Will implement any recommendations made by regulators and provide employee training. • Will offer credit monitoring to affected individuals and work to reimburse members.
Steps taken to notify individuals of the incident	On March 26, 2019, the Organization notified all members about the breach. The Organization reported that upon completion of its investigation it "…intends to notify affected …members in accordance with [PIPA]…. [and] this will take place within the next couple of weeks."

<table>
<tr><th colspan="2">REAL RISK OF SIGNIFICANT HARM ANALYSIS</th></tr>
<tr><td>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.</td><td>The Organization reported:

The risks that could potentially result from these incidents relate to fraud, financial loss, and identify theft.

I agree with the Organization’s assessment. A reasonable person would consider that the contact, identity and financial information at issue could be used to cause the significant harms of identity theft, fraud and financial loss.</td></tr>
<tr><td>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.</td><td>The Organization reported that its

…top priorities are to mitigate any financial loss to affected members and any harms that could result from the unauthorized access and misuse of personal information.

… members will be made whole financially for any losses resulting from the scheme.

At this point in time, [The Organization] is not aware of the whereabouts of the four missing …members' physical files. While [The Organization] believes that the Employee's only objective was to fraudulently divert funds, and there is no reason to believe that the Employee engaged or planned to engage in identity theft, if the whereabouts of the missing physical files are not determined, identify theft could be a risk.

In my view, a reasonable person would consider that the likelihood of identity theft and fraud resulting from this incident is increased because it resulted from deliberate, malicious action (theft and unauthorized diversion of funds). The fraudulent transactions took place over many years before being discovered. The physical files have not been recovered and their whereabouts are unknown.</td></tr>
<tr><th colspan="2">DECISION UNDER SECTION 37.1(1) OF PIPA</th></tr>
<tr><td colspan="2">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, identity and financial information at issue could be used to cause the significant harms of identity theft, fraud and financial loss. The likelihood of identity theft and fraud resulting from this incident is increased because it resulted from deliberate, malicious action (theft and unauthorized diversion of funds). The fraudulent transactions took place over many years before being discovered. The physical files have not been recovered and their whereabouts are unknown.</td></tr>
</table>

I require the Organization to notify the affected individuals whose personal information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand that, on March 26, 2019, the Organization notified all members about the breach and, upon completion of its investigation it "…intends to notify affected …members in accordance with [PIPA]…. [and] this will take place within the next couple of weeks."

I require the Organization to confirm to my office in writing, within 10 days of the date of this decision, that affected individual have been notified in compliance with the Regulation.

Jill Clayton
Information and Privacy Commissioner