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	Teck Highland Valley Cooper Corporation (Organization)
Decision number (file number)	P2020-ND-093 (File #015003)
Date notice received by OIPC	June 25, 2019
Date Organization last provided information	July 14, 2020
Date of decision	September 2, 2020
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 incident involved all or some of the following information: • name (retired member, beneficiary), • address, • date of birth, and • the name of the registered pension plan (hourly-paid employees or salaried employees). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	

Description of incident	• On June 12 and June 13, 2019, due to an incorrect mall merge operation, pension benefit statements sent to former employees were sent to the wrong addresses. • The breach was discovered on June 17, 2019 when some individuals who received the statements contacted the Organization to advise of the error. • The Organization wrote to the individuals who received the wrong letters and requested they return them to the Organization using an enclosed pre-addressed, stamped envelope. • The Organization reported, "Out of the 24 people in Alberta who were impacted, 13 confirmed that they either destroyed the letter or returned the document to us. Overall, over 80% of members either returned the letters to us or confirmed that they have shredded it." • The Organization reported that it does not have any indication that there has been any actual access to or misuse of the personal information.
Affected individuals	The incident affected 792 individuals of which 24 were residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Sent letters to all affected members who had received the wrong pension plan statement. • Requested the unintended recipients securely destroy the document or return it to the Organization. • Issued correct pension plan statements to members. • Taking steps to ensure similar mailings are reviewed by two people before being sent out and addresses are compared to those on file. • Notified privacy and financial regulators.
Steps taken to notify individuals of the incident	On June 19, 2019, affected members who received another's pension plan statement were notified by letter. The United Steel Workers Local 7619 notified former employees verbally on June 19, 2019 and by letter on June 21, 2019. The union posted information on their Facebook page to notify affected members. Local 7619 also posted the breach information in a closed Facebook post to alert retirees and raise awareness.
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	The Organization reported, *The disclosure of name and date of birth may be regarded as creating some risk of identity theft... We regard the information as moderately sensitive. No personal, financial or other*

also be "significant." It must be important, meaningful, and with non-trivial consequences or effects.	*identifying information was disclosed...We regard the identified harm as significant. [The Organization] does not have any indication that there has been any actual access to or misuse of the personal information. Because the persons to whom statements were sent were retirees …whose own personal Information has been inadvertently transmitted to others and because most of these persons have been requested to securely destroy or return the document … there arguably is less risk of these individuals taking advantage of the information they received.* In my view, a reasonable person would consider that the contact and identity information, along with the pension plan statement could be used to cause the significant harms of identity theft and fraud.
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 as follows: *Somewhat significant - information is sensitive, long exposure - the statement may not be returned or could be kept by the incorrect recipient for some time before being [returned]. There is no evidence of malicious intent or purpose. These are seniors, but not youth involved....* In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is decreased as the breach resulted from human error and not malicious intent. However, not all unintended recipients confirmed with the Organization that they securely destroyed or returned the information to the Organization. Although the Organization said it "does not have any indication that there has been any actual access to or misuse of the personal information", this does not necessarily mitigate the potential harm that may result if the information were to be used for fraudulent purposes, for example. Identity theft can happen months and even years after a data breach.
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 individuals. A reasonable person would consider that the contact and identity information, along with the pension plan statement could be used to cause the significant harms of identity theft and fraud. The likelihood of harm resulting from this incident is decreased as the breach resulted from human error and not malicious intent. However, not all unintended recipients confirmed with the Organization that they securely destroyed or returned the information to the Organization. Although the Organization said it "does not have any indication that there has been any actual access to or	

misuse of the personal information", this does not necessarily mitigate the potential harm that may result if the information were to be used for fraudulent purposes, for example. Identity theft can happen months and even years after a data breach.

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 the Organization notified members who received the wrong pension plan statement by letter on June 19, 2019. It is not clear, however, if the Organization notified the affected individuals (those individuals whose personal information was sent to another individual).

The Organization also said former employees were notified of the incident by Local 7619. The Organization did not provide my office with a copy of the notification sent by Local 7619.

Section 34.1 of PIPA says that "An organization having personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure."

Pursuant to section 37.1(1) of PIPA, where an organization is required to provide notice under section 34.1, I "may require the organization to notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure...".

The onus for notifying affected individuals about this incident rests with the Organization under PIPA, not the union and/or Local 7619. Further, it is not clear what affected individuals may have been told about the incident, and whether the information provided to them by the union and/or Local 7619 meet the requirements of section 19.1 as set out in the *Personal Information Protection Regulation.*

I require the Organization to confirm to my Office, within ten (10) days of the date of this decision, that all affected individuals whose personal information was collected in Alberta have been notified of this incident in accordance with the requirements outlined in the Regulation.

Jill Clayton
Information and Privacy Commissioner