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 Pipelines Ltd. (Organization)
Decision number (file number)	P2016-ND-42 (File #000032)
Date notice received by OIPC	December 5, 2014
Date Organization last provided information	December 5, 2014
Date of decision	August 16, 2016
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 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. In reporting this incident, the Organization noted that it "is normally a federally regulated company subject to [the *Personal Information Protection and Electronic Documents Act*] PIPEDA. However, one of the impacted individuals was slated to work in an unregulated (i.e. provincially regulated) part of our company." Although "the position would be in Ontario", the Organization noted that all applicants are Albertans.
Section 1(1)(k) of PIPA "personal information"	Some or all of the following information is at issue: • name, • home address, • details of position offered, • starting salary, • date of birth, • social insurance number,

	• basic tax amounts claimed, • citizenship, • emergency contact name and telephone number, • Authorization for Direct Deposit of Pay form (including name and bank account number) This information is "personal information" as defined in section 1(1)(k) of PIPA and was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• On three separate occasions (November 14, 18 and 21, 2014) an Administrator with the Organization inadvertently sent an email with a link to documents containing some or all of the information at issue to the wrong email address. • On the first occasion, the information included name, home address, details of position offered, and starting salary. • On the second and third occasions, the information included completed TD1 and TD1A taxation forms, with name, home address, date of birth, social insurance number, basic personal amounts claimed, and the Organization's New Hire Data Form containing addresses and contact information, citizenship, and date of birth. • The Organization discovered the breach on December 3, 2014.
Affected individuals	Two (2) individuals were affected by the incident.
Steps taken to reduce risk of harm to individuals	• The unintended recipient was asked to delete the emails in question and advise the Organization by return email that this was done. No reply was received. • Deleted the linked documents so they can no longer be accessed. • Recommended that affected individuals contact their banks and credit card companies to advise them of the situation. • The Organization is in the process of obtaining credit monitoring for the individuals.
Steps taken to notify individuals of the incident	Affected individuals were notified by telephone on December 5, 2014.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm	The Organization reported that "The potential harm in the first

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.	incident is relatively low. The only information exposed was name, home address, role, and offered salary. The potential harm that may result in the second and third incidents is significant. The most serious/likely harms would be financial loss, fraud, identity theft, and negative effect on credit records." I agree with the Organization. The personal information involved in the first incident does not include sensitive identity or financial information and could not be used to cause significant harm. The information involved in the second and third incidents, however, does include sensitive identity and financial information. This information could be used to cause the harms of identity theft, fraud, financial loss and negative effect on credit records. 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 the likelihood of harm resulting from the first incident was relatively low, considering the low sensitivity of the information exposed. However, the likelihood of harm resulting from the second and third incidents is "potentially high". The Organization noted that it does not know if the emails were opened or viewed by the unintended recipient and is not able to verify who may have accessed the documents or when. Further, "The information was not purposely hacked or stolen. The ability to access was sent inadvertently. We do not know that the recipient, even if they had actually accessed the information, had any criminal intent." I agree with the Organization's assessment. I have already found that the information involved in the first incident could not be used to cause significant harm. Therefore, there is no real risk of this occurring. Information involved in the second and third incidents however, could be used to cause significant harm. Although the incidents were the result of human error and not malicious intent, I nonetheless find there is a real risk of harm occurring. The Organization emailed the unintended recipient to request the emails be deleted but did not receive any response. Further, the Organization is not able to verify who may have accessed the documents or when.

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 affected individuals as a result of the second and third incidents. The information involved includes sensitive identity and financial information. This information could be used to cause the significant harms of identity theft, fraud, financial loss and negative effect on credit records. Although the incidents were the result of human error and not malicious intent, I nonetheless find there is a real risk of harm occurring. The Organization emailed the unintended recipient to request the emails be deleted but did not receive any response. Further, the Organization is not able to verify who may have accessed the documents or when. I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the Organization notified affected individuals by telephone on December 5, 2014 in accordance with section 19.1 of the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner