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	Syncrude Canada Ltd. (Organization)
Decision number (file number)	P2019-ND-027 (Files #006776 and 006839)
Date notice received by OIPC	October 10, 2017
Date Organization last provided information	August 31, 2018
Date of decision	February 19, 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 the individuals 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)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The following information was involved in this incident: • name, • address, • personal telephone number, • pension information, • basic and supplemental retirement account balances, • date of birth, • gender, • marital status, • social insurance number, • scans of government issued ID, • compensation and financial information, • salary, • pension payments, • LIRA or RRSP account information, • banking information, • employment information (hire date, termination date, years of service), and • spousal and beneficiary information.

	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	• On October 6, 2017, an employee of the Organization reported that that they had incorrect access permissions to an internal network directory, allowing the employee access to personal information of other employees. • A comprehensive investigation followed and found that there were four (4) unique exposures allowing unauthorized access to various folders between March 2, 2017 and October 13, 2017. • The Organization's IT support services are provided by an external service provider. There is a procedure for granting access requests, however the procedure was not followed. • The personal information was stored on secure servers in Alberta. The physical security of the server was not compromised.
Affected individuals	The Organization reported that 18,230 individuals were affected by the breaches. Affected individuals included employees (active, past, retired) and spouses (including those of deceased employees).

Steps taken to reduce risk of harm to individuals	• Access permissions were changed to end exposure and potential unauthorized access.
	• Appropriate access was re-established on folders.
	• After the investigation found more folders with incorrect permissions the server was shut down to correct the access permissions to the files and server.
	• Affected individuals were notified electronically and by mail.
	• Offered free credit bureau monitoring and alerts, credit reports and ID theft restoration services to affected individuals.
	• Established a telephone line for individuals who wished to discuss the matter further and /or had additional questions.
	• The IT service provider:
	  o Scanned all emails and found zero items sent internally or externally had any relevant file names.
	  o Completed a security scan of all "North America" LAN workstations looking for specific file names. There were zero results.
	  o Reported to the Organization that there was no sign of data on black market and no evidence of an external breach.

	• Affected server was turned off and information moved to high security file servers. IT processes have been changed to ensure risks related to the incidents do not reoccur. New servers will replace legacy servers. • The IT Service Provider has reinforced Management of Change practices with relevant Teams including a review of application control framework, change management practices and review of appropriate expected documentation in incident tickets/work orders including work plans. • The Organization will verify the IT Service Provider communicates and reinforces proper Management of Change compliance practices. • The Organization and IT Service Provider will work on a sensitive data incident protocol. • The IT Service Provider "proposes to perform a "cold eyes" health check of the Organization's computing environment."
Steps taken to notify individuals of the incident	The Organization notified approximately 18,200 affected individuals by electronic communication on October 16, 2017 and individual letter sent to their home address (mailed October 23, 2017). A Special Bulletin notification was posted on the employee portal and the retiree page of www.syncrudecentral.ca.
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 the "Potential harm is high due to the nature of the information and breadth of exposure." In my view, the contact, identity, employment and financial information at issue could be used to cause the significant harms of identity theft, fraud, financial loss and negative effects on credit reports, as well as hurt, humiliation, and embarrassment.
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 breaches are of low risk and moderate based on how difficult it would be for someone to access the personal information in the folder. The Organization also stated that "a scan of sent emails…showed zero items sent internally or externally with relevant file names" and there were "no signs of data on the black market, and no evidence of an external breach." In my view, a reasonable person would consider there is a real risk of harm resulting in this case. Although the Organization believes the incident did not result from malicious intent (but rather human error), and the individual who noticed the access permissions notified management, the Organization was not able to determine who else may have accessed the files over the time period. The

	Organization said a maximum of 849 could have accessed the files. The files were open to employees and for some folders this access was available for several months.

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.

The contact, identity, employment and financial information at issue could be used to cause the significant harms of identity theft, fraud, financial loss and negative effects on credit reports, as well as hurt, humiliation, and embarrassment. Although the Organization believes the incident did not result from malicious intent (but rather human error), and the individual who noticed the access permissions notified management, the Organization was not able to determine who else may have accessed the files over the time period. The Organization said a maximum of 849 could have accessed the files. The files were open to employees and for some folders this access was available for several months.

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 approximately the affected individuals by electronic communication on October 16, 2017 and individual letter sent to their home address (mailed October 23, 2017). A Special Bulletin notification was posted on the employee portal and the retiree page of www.syncrudecentral.ca. The Organization is not required to make further attempts to notify the affected individuals.

Jill Clayton
Information and Privacy Commissioner