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)	P2021-ND-220 (File #022833)
Date notice received by OIPC	August 20, 2021
Date Organization last provided information	September 20, 2021
Date of decision	November 8, 2021
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 operates in Alberta and 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, • date of birth, • banking information, • address, • social insurance number, • salary/rate information, • bonus payments, • legal deductions, • termination information (type), • T4s, • severance payments, • leave of absences, • WCB payments, • employee benefits (rental, relocation, housing, tuition), and • benefit contributions (Thrift, SRP, ECO, GRRSP, TFSA).

	This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization's information and technology support services are supplied by an external IT service provider. These services include the management of a server used by the Organization's payroll to store payroll files. • On August 11, 2021, an analyst with the Organization was performing testing and noticed improper server access settings, enabling access by all users with a LAN account logged into the network. • The improper server access settings were in place as early as June 2019 and were fully corrected on August 12, 2021. • The Organization reported that its investigation has not found any indication at this time that the information was accessed inappropriately.
Affected individuals	The incident affected approximately 13,000 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Resolved the security gap. • Reviewed and aligned the incorrect access to the approved security model. • Reviewing the remaining migrated servers against approved security models to ensure adherence.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter during the week of September 20, 2021.
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, *There is a risk that affected employees and ex-employees will be at increased risk of identity theft, fraud, financial loss and negative impact on credit records.* In my view, a reasonable person would consider that the contact, identity, employment and tax information at issue could be used to cause the significant harms of fraud, identity theft, financial loss and embarrassment or humiliation.

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, *Highest level of sensitivity due to Social Insurance Numbers and banking information being exposed.* *… preliminary investigation suggests that it is highly unlikely that anyone in fact accessed this information because the user would have to know the path to the server, which is not published. [The Organization] acknowledges that the risk cannot be fully discounted because it has not been possible to date to establish whether any unauthorized users accessed the information.* *However, there is no evidence to suggest that the information has been extracted or that there has been any malicious intent.* In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased, as the Organization conceded, "the risk cannot fully discounted because it has not been possible to date to establish whether any unauthorized users accessed the information". The lack of reported incidents resulting from this breach to date is not a mitigating factor, as identity theft and fraud can occur months and even years after a data breach. It appears the information at issue may have been exposed for two (2) years. Lastly, given the potential for personal/professional relationships involving employees, humiliation and embarrassment are real risks.

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, identity, employment and tax information at issue could be used to cause the significant harms of fraud, identity theft, financial loss and embarrassment or humiliation.

The likelihood of harm resulting from this incident is increased, as the Organization conceded, "the risk cannot fully discounted because it has not been possible to date to establish whether any unauthorized users accessed the information". The lack of reported incidents resulting from this breach to date is not a mitigating factor, as identity theft and fraud can occur months and even years after a data breach. It appears the information at issue may have been exposed for two (2) years. Lastly, given the potential for personal/professional relationships involving employees, humiliation and embarrassment are real risks.

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 affected individuals by letter during the week of September 20, 2021, in accordance with the Regulations. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner