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	JTI-Macdonald Corporation (Organization)
Decision number (file number)	P2021-ND-016 (File #016439)
Date notice received by OIPC	July 13, 2020
Date Organization last provided information	January 25, 2021
Date of decision	February 16, 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 the 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 a Canadian entity and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • internal employee ID number, • job title, • start date of role, • gender, • client attribution code, • annual salary, • salary range, • short and long term bonus information, and • work office location (by postal code). The Organization reported that the exposed data set does not include name, email address, social security number or government identification number, nor credit card or bank account information. However, the dataset does include employee ID number. Given this, the information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent this information was collected in Alberta, PIPA applies.

DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• The Organization provides salary compensation information to its service provider, Korn Ferry, on an annual basis. • On June 26, 2020, Korn Ferry learned through a blog post by a security researcher, that an Amazon Web Services S3 Server (AWS S3 Server) contained data submitted to Korn Ferry by the Organization related to 2018 salaries. • The data was inadvertently made publicly available on the AWS S3 Server on July 24, 2019 and was removed on June 26, 2020. • The Organization was initially notified of the breach on July 1, 2020. On July 10, 2020, the Organization was informed by Korn Ferry that it assumes that the information has likely been viewed and/or downloaded and has no reason to believe the security researcher is incorrect. • The Organization reported that Korn Ferry does not know whether the data was viewed or downloaded because logging was not enabled on the AWS Server. • The security researcher identified an actor operating on the dark web selling access to the data. The security researcher claims to have acquired the information sold by the actor.
Affected individuals	The incident affected 112 individuals, including 2 whose personal information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	Organization: • Notified affected individuals. • Providing credit monitoring for 12 months to affected individuals. Korn Ferry: • Reviewing and tightening its internal permission protocols. • Reviewing internal procedures for the creation and management of test data.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on July 13, 2020

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 that the possible harms that may occur as a result of the breach are "Risk of identity theft, phishing schemes, etc.". I agree with the Organization's assessment. A reasonable person would consider that the employee information at issue could be used to cause the significant harms of identity theft and for phishing purposes, increasing vulnerability to 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 reported it … *… has concluded there is a real risk of significant harm as we believe this data was exfiltrated by an unknown actor who may have attempted to sell it on the dark web. [The Organization] is unaware of the extent that this information may have been shared. If acquired by a nefarious actor, it may be used to harm affected individuals.* I agree with the Organization's assessment. A reasonable person would consider the likelihood of harm resulting from this incident is increased because the information was exfiltrated by an unknown actor who attempted to sell it on the dark web. The Organization does not know whether the data was viewed or downloaded. In addition, the information may have been exposed for approximately eleven (11) 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.

A reasonable person would consider that the employee information at issue could be used to cause the significant harms of identity theft and for phishing purposes, increasing vulnerability to identity theft and fraud.

The likelihood of harm resulting from this incident is increased because the information was exfiltrated by an unknown actor who attempted to sell it on the dark web. The Organization does not know whether the data was viewed or downloaded. In addition, the information may have been exposed for approximately eleven (11) 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 affected individuals in an email dated July 13, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner