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	Tenaris Group / TMK IPSCO Canada Ltd. (the Organizations)
Decision number (file number)	P2020-ND-064 (File #015396)
Date notice received by OIPC	March 9, 2020
Date Organization last provided information	March 9, 2020
Date of decision	July 13, 2020
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organizations are 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"	Tenaris Group acquired TMK IPSCO in January 2020 (acquisition in Canada and US). Tenaris Group and TMK IPSCO are "organizations" 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, • home address, • social security number/social insurance number, • annual salary, • date of birth, and • benefits and/or life insurance coverages, all as of October 15, 2019. 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	• TMK IPSCO was acquired by the Tenaris Group in January 2020. Following the close of the transaction, Tenaris performed an internal control assessment and, on January 28, 2020, identified a lack of security controls for certain files stored in a temporary storage location. • These files were potentially accessible by all the acquired Organization's employees.
Affected individuals	The incident affected 32 individuals.
Steps taken to reduce risk of harm to individuals	• Restricted access to authorized users only to both the server containing the temporary storage location and the temporary storage location. • Implemented appropriate access restrictions. • Implementing IT security policies and procedures for all of the acquired Organization's resources and information.
Steps taken to notify individuals of the incident	The Organization did not report notifying affected individuals.
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 "Due to the sensitive and unchanging nature of some of the exposed personal information date of birth, SIN, etc.) affected individuals may be subject to identity theft or fraud." In my view, a reasonable person would consider the contact, identity, employment and insurance information at issue could be used to cause the significant harms of identity theft and fraud. Salary information could also be used to cause hurt, humiliation and embarrassment, as well as damage to relationships. 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, *Although the exposed information is sensitive information and could result in the harm identified above, the chance that the exposed information was accessed by an unauthorized individual is low. The unauthorized individual would have had to have knowledge of the exact location of these files or how to perform the same system scan performed by the IT Audit department, which ultimately identified the lack of security controls. As of the date of this notification, here [sic] is no evidence to indicate that any information contained in these files was accessed or used by any unauthorized individual.*

	The Organization also reported that, to its knowledge, there has been "…no claim, report or concern" by any of the potentially affected individuals. In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is decreased because the personal information was compromised due to human error and not malicious action of an unknown third party. However, the Organization did not report how long the information was exposed. Further, although the Organization said there is "no evidence to indicate that any information contained in these files was accessed or used by any unauthorized individual", it did not report any technical controls (such as audit logs) that could evidence that the information was not accessed. The lack of reported harms or concerns to date does not mitigate against future harms occurring.

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 the contact, identity, employment and insurance information at issue could be used to cause the significant harms of identity theft, and fraud. Salary information at issue could also be used to cause hurt, humiliation and embarrassment, as well as damage to relationships. These are significant harms.

The likelihood of harm resulting from this incident is decreased because the personal information was compromised due to human error and not malicious action of an unknown third party. However, the Organization did not report how long the information was exposed. Further, although the Organization said there is "no evidence to indicate that any information contained in these files was accessed or used by any unauthorized individual", it did not report any technical controls (such as audit logs) that could evidence that the information was not accessed. The lack of reported harms or concerns to date does not mitigate against future harms occurring.

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) and **confirm to my Office in writing, within ten (10) days of the date of this decision, that affected individuals have been notified of this incident in accordance with the requirements outlined in the Regulation.**

Jill Clayton
Information and Privacy Commissioner