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	TGS Canada Corp. (Organization)
Decision number (file number)	P2019-ND-136 (File #012646)
Date notice received by OIPC	March 27, 2019
Date Organization last provided information	March 27, 2019
Date of decision	August 13, 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 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 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: • name, • income for the year, • income tax deducted (paid), • CPP contributions, • EQPP contributions, • El premiums paid, • home address, • social insurance number, • taxable benefits included in the employee's compensation. 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 February 26, 2019, the Organization was advised by one of its vendors of a security incident and that some of the vendor's data may have been stolen. • On February 28, 2019, the vendor confirmed to the Organization that a former employee had stolen certain data from the vendor's computer network. It remained unknown to the Organization at that time whether the Organization's data was among the data stolen by the former employee. • On March 15, 2019, the vendor confirmed that the Organization's data was among the client data stolen. • The Organization has since learned that on February 22, 2019, the vendor was notified that one of its independent contractors had received a text message from an unidentified individual stating that the individual had gained access to and downloaded the vendor's client data. On February 27, 2019, the vendor determined that a former employee had surreptitiously and unlawfully downloaded data from the vendor's network to a remote server during his short-term employment from January 28, 2019 to February 20, 2019). • The former employee has since been arrested and charged.
Affected individuals	The incident affected up to 3,000 individuals, including 23 current and former employees of the Organization; 16 of the 17 current employees reside in Alberta; the other employee has since been transferred.
Steps taken to reduce risk of harm to individuals	The Organization: • Hosted a town hall with all employees regarding the incident where the circumstances of the incident were discussed and any questions answered. • Offered identity theft and credit monitoring services to the affected individuals for a minimum period of one year. • Reviewing its agreements with service providers to ensure adequate data protection and security safeguards regarding personal information provided to service providers. The Organization reported that its vendor: • Reported to law enforcement and data protection authorities. • Changed passwords on systems, devices and applications. • Shut down any remote access capability. • Ongoing monitoring of inbound and outbound traffic from its systems. • Investigated to determine the scope of the individual's wrongdoing; and engaged third-party forensic consultants to assist with the investigation.

Steps taken to notify individuals of the incident	Affected individuals were notified in writing on March 25, 2019.
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 "…since the information … involved in the incident include [sic] highly sensitive personal and financial information, there is a risk of identity theft, fraud and financial loss to the employees in question, in addition to humiliation and embarrassment having employment compensation information potentially disclosed." I agree with the Organization's assessment. A reasonable person would consider that the identity, tax and employment information at issue could be used to cause the significant harms of identity theft and fraud, 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 likelihood that harm could result … is moderate to high. The personal information involved in the Incident is highly sensitive, and it would not be difficult for this information to be used for the purposes of identity theft and fraud….the [vendor's] employee has been arrested and the stolen data has been located.* *[The Organization] further understands that there is currently no evidence one way or another indicating that the information of [the Organization's employees] was further disseminated or disclosed prior to being recovered.* *The fact that the Incident was caused as a result of the theft of the information by a former …employee (malicious intent) increases the likelihood that harm could result to the affected individuals.* *As noted below, both [the Organization and its vendor] have taken several steps to minimize the likelihood of harm from the Incident.* In my view, a reasonable person would consider that the likelihood of identity theft and fraud resulting from this incident is increased because it resulted from deliberate, malicious action (theft). The information was apparently unlawfully downloaded over the course of almost a month; it is not clear how long after this that the former employee was arrested. Although the Organization reported there is no evidence the information was further disseminated or disclosed prior to being recovered, this is not known for sure.

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 identity, tax and employment information at issue could be used to cause the significant harms of identity theft and fraud, as well as hurt, humiliation and embarrassment. The likelihood of identity theft and fraud resulting from this incident is increased because the breach was the result of deliberate, malicious action (theft). The information was apparently unlawfully downloaded over the course of almost a month; it is not clear how long after this that the former employee was arrested. Although the Organization reported there is no evidence the information was further disseminated or disclosed prior to being recovered, this is not known for sure. 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 that affected individuals were notified in writing on March 25, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner