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	TGSI Canada Corp. (Organization)
Decision number (file number)	P2021-ND-077 (File #012380)
Date notice received by OIPC	March 4, 2019
Date Organization last provided information	April 10, 2019
Date of decision	March 9, 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 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, • address, • social insurance number, • salary information, • income tax information, and • other withholding information listed on tax documents. 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	• The Organization is a specialized Chartered Accountancy practice and provides tax consulting services to various clients. • On February 22, 2019, the Organization was notified that one of is independent contractors had received a text message from an unidentified individual stating that the individual had

	gained access to and downloaded the Organization's client data. • The Organization took precautionary steps and changed all passwords for its remote access capabilities and locked down its servers. • On February 25, 2019, the Organization was notified by seven (7) clients that they had received a suspicious email from an unidentified individual claiming to have stolen their "client data including project reports, emails, audits, financial statements etc." from the Organization. The email did not provide proof that the client data was in the individual's possession. The email asked the recipients to name a price for the data not to be published. • On February 27, 2019, the Organization determined that a former short-term employee had unlawfully downloaded data from the Organization's network to a remote server between January 28, 2019 and February 20, 2019. • The Organization determined that individuals affected by this incident are employees of its clients. • The former employee has since been arrested and charged.
Affected individuals	The incident affected approximately 3,000 individuals.
Steps taken to reduce risk of harm to individuals	• Investigated with assistance of third party forensic consultants. • 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. • Engaged external legal counsel. • Installed additional security and monitoring software. • Will provide updated training to employees about cybersecurity risks. • Reviewed policies to help combat risks in the future. • Ordered and paid for 12 months of credit monitoring services and identity theft insurance for affected individuals. • Communicated internally with all employees so they are aware of the incident, can assist clients, individuals and the public with any inquiries. • Destroyed all existing magnetic access passes and issued new ones to employees. • Changed office access protocols. • Enhanced procedures for data cleansing and data storage. • Engaged a cybersecurity firm to guide the Organization's cybersecurity practices and processes moving forward and conduct regular audits of the Organization's systems.

	• Will conduct criminal records checks for all new hires moving forward, in accordance with applicable law.
Steps taken to notify individuals of the incident	The Organization determined in conjunction with its clients that the most efficient way to notify affected individuals was for the clients to provide the individuals with such notice directly. On March 6, 2019, the Organization developed a notification letter for its clients to use for this purpose.
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 primary risks that could potentially result from this incident, depending upon the personal information that may be determined to have been stolen, are those related to fraud, financial loss and identity theft." 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, "To date, the extortion attempts have been directed at companies and not individuals and it is hoped that the quick identification of the employee and the CPS' plans to execute a search warrant will prevent further such attempts. However, there is currently a risk of similar extortion or other financial impacts to affected individuals As noted below, [the Organization] has taken several steps to minimize the likelihood of harm from this 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 approximately one month. Although the Organization reported that following the employee's arrest, neither the Organization nor its clients have received any further emails or demands from third parties with respect to this incident, the Organization can only speculate that the information was not further disseminated or disclosed prior to being recovered.
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 it resulted from deliberate, malicious action (theft). The information was apparently unlawfully downloaded over the course of approximately one month. Although the Organization reported that following the employee's arrest, neither the Organization nor its clients have received any further emails or demands from third parties with respect to this incident, the Organization can only speculate that the information was not further disseminated or disclosed prior to being recovered.

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 reported that it determined in conjunction with its clients that the most efficient way to notify affected individuals was for the clients to provide the individuals with such notice directly. Further, the Organization developed a notification letter for its clients to use for this purpose.

The Organization is not required to notify the affected individuals again if they have already been notified. However, as the Organization asserts that it had control of the personal information at issue, I require it to confirm to my office, within 10 days of the date of this decision, that all affected individuals were notified in accordance with the Regulation.

Jill Clayton
Information and Privacy Commissioner