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	Geo Logic Systems Ltd. (Organization)
Decision number (file number)	P2021-ND-078 (File #012589)
Date notice received by OIPC	March 6, 2019
Date Organization last provided information	March 6, 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, • home address, • annual (2018) salary and additional compensation, • income tax, and • other withholding information. 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 25, 2019, a third party contractor notified the Organization that a data breach had occurred which consisted of unauthorized access to personal information.

	• The contractor determined that an individual downloaded certain data from the contractor which included the Organization's employee information.
Affected individuals	The incident affected 58 individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	The Organization: • Hosted a town hall with all employees to discuss the incident and answer questions. • 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	The Organization's vendor drafted a notification about the incident and the Organization notified affected individuals in writing on March 4-5, 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 that "Personal information could be utilized by unauthorized parties." In my view, a reasonable person would consider that the contact, employment and tax 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	The Organization reported that "Harm is possible, however Risk Mitigation efforts should prevent this. We have been informed that the Calgary Police Service has identified and arrested the responsible individual and the data has been recovered." In my view, a reasonable person would consider that the likelihood of identity theft and fraud resulting from this incident is increased

between the incident and the possible harm.	because it resulted from deliberate, malicious action (theft). The information was apparently unlawfully downloaded over the course of almost a month. As well, there is no evidence 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 contact, employment and tax 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 almost a month. As well, there is no evidence 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 that the Organization's vendor drafted a notification about the incident and the Organization notified affected individuals in writing on March 4-5, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner