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	Geokinetics Inc. (Organization)
Decision number (file number)	P2017-ND-133 (File #005247)
Date notice received by OIPC	March 14, 2017
Date Organization last provided information	March 14, 2017
Date of decision	October 2, 2017
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 pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization has its head office in Houston, Texas, and an office in Calgary, Alberta. 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 all or some of the following information: • name, • address, • social insurance number, and • earning information (wage, salary, 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 January 25, 2017, an employee with the Organization received an email that was purportedly a request from the Organization's President and CEO for 2016 U.S. IRS Forms W-2 (W-2).

	• Believing the email was legitimate, the employee replied to the message and attached the W-2s. • On March 6, 2017, the Organization discovered that the W-2s were sent outside the organization as part of a spear phishing email scam.
Affected individuals	The incident affected 6 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Investigated the incident and analyzing where process changes are needed. • Offered affected individuals free one-year membership in credit monitoring and identity theft protection services. • Recommended that affected individuals remain vigilant for incidents of fraud or identity theft by reviewing their accounts statements. • Notified the IRA and state taxing authorities of the incident who will monitor affected employees' returns for fraudulent activities.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on March 7, 2017 and provided written notification via mail on March 14, 2017.
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 information "could be used to attempt to purpetrate [sic] fraud or identity theft." I agree with the Organization that the contact, identity, and financial information at issue could be used to cause the significant harms of fraud and identity theft.
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 it has "notified the IRS and state taxing authorities" and they "will monitor affected employees' returns for the purpose of preventing fraudulent tax refunds being paid out." The Organization said it "is aggressively analyzing where process changes are needed and will take appropriate steps." In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (a spear phishing email scam). Further, the information may have been exposed for approximately one and a half 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. The contact, identity, and financial information at issue could be used to cause the significant harms of fraud and identity theft. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (a spear phishing email scam). Further, the information may have been exposed for approximately one and a half months. I require the Organization to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the Organization notified affected individuals by email on March 7, 2017 and later by mail on March 14, 2017, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner