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	geoLogic Systems (Organization)
Decision number (file number)	P2017-ND-38 (File #005036)
Date notice received by OIPC	February 16, 2017
Date Organization last provided information	February 16, 2017
Date of decision	March 3, 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 is based in Calgary, Alberta and is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	Some or all of the following information was involved in this incident: • name, • business title, • business address, • business telephone number, • business email address, • email contents related to corporate and business activities and transactions, and • for one individual, a resume (including home telephone number, address, and presumably education and employment history). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta.

	Section 4(1) of PIPA says "Except as provided in this Act and subject to the regulations, this Act applies to every organization and in respect of all personal information." Section 4(1)(d) of PIPA says that the Act does not apply to the collection, use and disclosure of business contact information "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." Section 1(1)(a) of PIPA defines business contact information to mean "an individual's name, position name or title, business telephone number, business address, business e-mail address, business fax number and other similar business information." Much of the information at issue appears to qualify as "business contact information". However, this information, in conjunction with email contents related to corporate and business activities and transactions is more than just business contact information. Further, I considered the circumstances of the incident, whereby an email account was compromised so that an unauthorized individual was able to forward and access the business contact information and email contents. In my view, this unauthorized access to and use of the information, including business contact information, was not "for the purposes of enabling [affected individuals] to be contacted in relation to the individual's business responsibilities and for no other purpose." Therefore, I find that PIPA applies in this matter.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On December 20, 2016, an unknown individual accessed the email account of the Organization's CEO and established a "mail forward" function such that all emails delivered to the account were forwarded to an unauthorized Gmail email account. • The Organization reported "The content of the e-mails and the various attachments related to corporate and business activities and transactions" and some of it was innocuous, consisting of read receipts, and newsletter subscriptions. Some were internal company emails. • The incident was discovered on January 3, 2017 when an email which was too large to be received by the unauthorized account bounced back. • An evaluation of the Organization's system showed no evidence of malware, keyloggers or foreign programs or bots.
Affected individuals	The Organization reported emails from 610 different email addresses were forwarded.

Steps taken to reduce risk of harm to individuals	• Conducted a full system evaluation and regularly monitoring system to identify any changes to the webmail interface. • Changed passwords, and enhanced password and identity requirements. • Notified law enforcement and the Organization's bank.
Steps taken to notify individuals of the incident	Affected individuals have not been notified.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to the 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 "If there is a risk of harm in this incident, it is the potential harm of phishing." Nonetheless, the Organization reported its "view that the business contact information involved in this incident does not lend itself to phishing" for a number of reasons including the "relatively small" number of affected individuals and because the "common nexus uniting the affected individuals is that their respective companies did business with [the Organization]. The nature of the information disclosed does not lend itself to a mass e-mail phishing attack given that factor uniting the group is tenuous." In my view, the email addresses at issue along with email contents related to corporate and business activities and transactions, and knowing individuals associated with this personal information have a common nexus of doing business with the Organization, could be used to cause the significant harm of phishing, thereby exposing the affected individuals to other potential harms, despite the "relatively small" number of affected email addresses. Comprehensive profile information included in a resume (contact, educational and employment history) could also be used for identity theft and fraud, which 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.	As noted above, the Organization assessed the likelihood of harm resulting from this incident to be low for a number of reasons, including the "relatively small" number of email addresses affected, and the "tenuous" nexus uniting affected individuals. Further, the Organization reported "there is no evidence that any specific information was being sought." In my view, the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion and misdirection of email) and the information was exposed for 2 weeks before the incident was discovered. The Organization did not report that the unauthorized individual responsible had been identified.

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 as a result of this incident. The email addresses at issue along with email contents related to corporate and business activities and transactions, and knowing individuals associated with this personal information have a common nexus of doing business with the Organization, could be used to cause the significant harm of phishing, thereby exposing the affected individuals to other potential harms despite the "relatively small" number of affected email addresses. Comprehensive profile information included in a resume (contact, educational and employment history) could also be used for identity theft and fraud, which are significant harms. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion and misdirection of email) and the information was exposed for 2 weeks before the incident was discovered. The Organization did not report that the unauthorized individual responsible had been identified. I require the Organization to notify affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation) and provide me with written confirmation that it has done so on or before March 17, 2017.

Jill Clayton
Information and Privacy Commissioner