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	Guardian Law Group LLP (Organization)
Decision number (file number)	P2020-ND-033 (File #013861)
Date notice received by OIPC	November 15, 2019
Date Organization last provided information	November 22, 2019
Date of decision	March 9, 2020
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 all or some of the following information: • name (possibly), and • email address. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. Some of the information may qualify as "business contact information" which is defined in section 1(1)(a) of PIPA 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." 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."

	In this case, I considered that the possible unauthorized access to the information was not "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." As a result, PIPA applies to the business contact information.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On November 13, 2019, the Organization was contacted by another law firm who reported it had received a suspicious email that appeared to have been sent from the Organization. The email was sent from an address that was the actual email address of an employee of the Organization who was on vacation at the time. • The Organization investigated and found that "spam emails" had been sent from an Organization email account. • The Organization was contacted by about 60 individuals and companies regarding the emails. • The Organization traced the IP address to Japan where the email account was accessed, which involved servers hosted by a company named Green Server. The Organization informed Green Server that one of its hosted IPs had been used to send email from a "hacked account" and requested they take action. Green Server informed the Organization that it terminated the virtual private server (VPS) and customer with the IP address in question.
Affected individuals	The incident affected approximately 400 individuals.
Steps taken to reduce risk of harm to individuals	• Provided instruction to employees regarding the incident and how to respond. • Informed individuals that the specific email was a scam and not to open the link. • Ran virus software and malware software to ensure nothing was implanted on the system. • Changed password for the internal email account. • IT/training improvements are required.
Steps taken to notify individuals of the incident	Affected individuals were notified by email sent on November 20 and 21, 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 "Individuals were sent spam emails from one of our companies [sic] email. A person who opens the email could assume it is safe and click on an unsafe link which could harm their computer." In my view, a reasonable person would consider that the email addresses could be used for phishing purposes, resulting in increased vulnerability to identity theft and fraud.
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 the significant harm will result is "Extremely low. Our office does not typically send emails with links." In my view, a reasonable person would consider that 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 (deliberate intrusion). The unauthorized access did in fact result in fraudulent emails being sent.

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.

In my view, a reasonable person would consider that the email addresses could be used for phishing purposes, resulting in increased vulnerability to identity theft and fraud. The likelihood of harm is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). The unauthorized access did in fact result in fraudulent emails being sent.

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 notified affected individuals by email on November 20 and 21, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner