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	Kearns, Brinen & Monaghan (Organization)
Decision number (file number)	P2020-ND-015 (File #013720)
Date notice received by OIPC	October 1, 2019
Date Organization last provided information	October 1, 2019
Date of decision	February 13, 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 the 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 information at issue includes: • name, • address, • social insurance number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• Two employees received a phishing email with a hyperlink. The employees clicked on the link, which took them to a site that looked like a genuine site. Each of the employees entered their credentials into the site. Once the threat actor had the credentials, he accessed the employees' emails and set up a forwarding rule.

	• The Organization reported the breach occurred on October 15, 2018 and was discovered on July 15, 2019 when suspicious activity was reported by an employee to the Organization's IT Service Provider, who investigated.
Affected individuals	The incident affected 444 individuals, including 13 in Alberta.
Steps taken to reduce risk of harm to individuals	• Instituted two factor authentication. • Installed more secure firewall. • Reviewed all servers, PCs, and systems for viruses. • Changed all passwords for domains and emails. • Instituted new password policy requirement passwords to be more complex. • Deleted all forwarding rules and disabled ability to set up forwarding rules to forward emails outside domain. • Set up alert when anyone logs into environment from new device or IP address. • Developed written procedures to follow when employee leaves, including resetting account, blocking sign-in, disabling domain account, changing phone login and remotely wiping all data from cell phone. • Regular audits of new security procedures.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on October 1, 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 did not specifically identify the potential harm(s) that might result from this incident but reported "We have no evidence that the information was misued [sic] in any way". In my view, a reasonable person would consider that the identity information at issue (social insurance number) could be used to cause the significant harms of 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 "Based on our assessment, we believe the likelihood of harm is low". In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased as it was the result of malicious intent (phishing and email forwarding rule). It appears the email account was exposed for approximately 9 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. A reasonable person would consider that the identity information at issue (social insurance number) could be used to cause the significant harms of identity theft and fraud. The likelihood of harm resulting from this incident is increased as it was the result of malicious intent (phishing and email forwarding rule). It appears the email account was exposed for approximately 9 months. 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 individuals were notified by notified by letter on October 1, 2019. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner