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	Power Survey and Equipment Ltd DBA Powerside (Organization)
Decision number (file number)	P2021-ND-190 (File #017728)
Date notice received by OIPC	October 9, 2020
Date Organization last provided information	June 9, 2021
Date of decision	October 14, 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 pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization operates in Alberta and 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: • first and last name, • business email address, • business physical address, • business telephone number and cell phone number, and • job title. The Organization reported that the above personal information is "all from personnel of customers and partners." This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. Some of the personal information appears to be 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 such, the information is not excluded from the Act, and PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• On August 10, 2020, the Organization received a suspicious phishing email from fraudsters impersonating an employee. • Upon learning of the incident on August 31, 2020, the Organization investigated. As a result of the investigation, the Organization believes that an unauthorized person breached its email security systems and accessed the email account of its employee. • The Organization's believes that the intruder had access to this employee's emails and contact information and set up an email forwarding rule, which allowed the intruder to send unauthorized emails to the employee's contacts. • The Organization reported that it cannot rule out the possibility that the intruder sent more unauthorized email messages but permanently deleted them which could not be traced forensically.
Affected individuals	The incident affected 874 Canadians, of which approximately 45 had their information collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Engaged a third-party security firm to initiate an investigation and contain the incident. • Implementing additional controls over its email systems and reminding employees of best practices.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on September 3, 2020.

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 any harm that might result from this incident, but its notification to affected individuals stated, • *Be alert to any requests for personal information, in particular financial information, account numbers or passwords. Always verify the identity of the requester. Most legitimate businesses will not require you to provide this information via email.* • *Use complex passwords, change your passwords frequently and do not use the same password across multiple accounts.* • *Confirm the sender's identity before replying to email requests and before opening attachments or clicking on links, even if they appear to come from a legitimate source.* • *Consult your Information Technology department about any phishing attempts.* • *Call us to validate communications originating from Powerside.* In my view, a reasonable person would consider that the contact information along with email address and association with the Organization could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These 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.	The Organization did not specifically provide an assessment of the likelihood that significant harm would result from this incident, although it reported, *"...we cannot rule out the possibility that the intruder sent more unauthorized email messages but permanently deleted them which could not be traced forensically."* 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 personal information at issue was used to send phishing emails.
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 information along with email address and association with the Organization could be used for the purposes of phishing, increasing vulnerability	

to identity theft and fraud. These are significant harms. 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 personal information at issue was used to send phishing emails.

I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified affected individuals by email on September 3, 2020. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner