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 Engineers, Inc. (Organization)
Decision number (file number)	P2021-ND-070 (File #016611)
Date notice received by OIPC	August 4, 2020
Date Organization last provided information	February 24, 2021
Date of decision	March 9, 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 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 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: • name, • social insurance number, • date of birth, • driver's license or state identification, • financial account information, and • health insurance information. 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	• On March 9, 2020, the Organization became aware of suspicious activity related to its email system. • The Organization investigated and determined that there was unauthorized access to certain email accounts between "December 19, 2010 and March 3, 2020". • The Organization reviewed the affected accounts and on June 25, 2020, determined that the email accounts contained some information related to individuals.
Affected individuals	The incident affected 3,406 individuals, including 8 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Investigated and responded to the incident. • Assessed the security of its systems. • Implemented additional safeguards. • Trained employees. • Provided access to credit monitoring services for twenty four (24) months to affected individuals. • Provided guidance to affected individuals on how to protect against identity theft and fraud.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on or about August 4, 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 the type of harm(s) that might result from this incident, but its notification to affected individuals stated the Organization... *... is providing you with access to twenty-four (24) months of credit monitoring and identity protection services ...at no cost to you. A description of services and instructions on how to enroll can be found within the enclosed Steps You Can Take to Protect Against Identity Theft and Fraud... You can also enroll to receive the complimentary credit monitoring and identity protection services ...* In my view, a reasonable person would consider that the contact, identity and financial information at issue could be used to cause the harms of identity theft, fraud, and financial loss. Medical information could be used to cause humiliation, hurt and embarrassment. These are all 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 report its assessment of the likelihood that significant harm would result from this incident. 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 (unauthorized access). Further, it appears the email account was exposed for at least seventy-five (75) days, if not longer.

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, identity and financial information at issue could be used to cause the harms of identity theft, fraud, and financial loss. Medical information could be used to cause humiliation, hurt and embarrassment. These are all 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 (unauthorized access). Further, it appears the email account was exposed for at least seventy-five (75) days, if not longer.

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 letter on or about August 4, 2020 in accordance with the Regulations. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner