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	Enhance Energy Inc. (Organization)
Decision number (file number)	P2022-ND-006 (File #022140)
Date notice received by OIPC	July 7, 2021
Date Organization last provided information	January 24, 2022
Date of decision	March 17, 2022
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, • email address, • employment information and, • contents of mailbox. 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 February 16, 2021, unauthorized users logged into the corporate email accounts of five of the Organization's employees. • A total of 32 suspicious logins were identified between February 16, 2021 and April 9, 2021.

	• On April 9, 2021, a failed attempt at wire fraud was discovered when a supplier of Enhance Energy inquired about a payment.
Affected individuals	The incident affected five (5) individuals whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Forced all users to log off and changed all passwords. • Disabled all mailbox rules. • Removed all administrator accounts except for one. • Use more complex passwords and multi-factor authentication. • Implementation of additional security measures is being discussed with the Organization's service provider and operations team.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on June 9, 2021.
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, *Possible harms that may be suffered by the individuals affected by the breach include: loss of control of personal information, identity theft, fraud and loss of confidentiality of information protected by professional secrecy.* In my view, a reasonable person would consider that email addresses, particularly in conjunction with name and employment information 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 reported the likelihood that the harm will result was "Low". 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 (phishing). Further, it appears the email account was exposed for approximately seven (7) weeks.
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 email addresses, particularly in conjunction with name and employment information 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 (phishing). Further, it appears the email account was exposed for approximately seven (7) weeks.

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 June 9, 2021, in accordance with the Regulations. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance