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	ENMAX Corporation (Organization)
Decision number (file number)	P2020-ND-180 (File# 015771)
Date notice received by OIPC	May 8, 2020
Date Organization last provided information	May 8, 2020
Date of decision	December 8, 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 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, • street address, • telephone number, • email address, • Organization's account number, and • payment deferral request. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• On March 29, 2020, the Organization was the target of a malicious spear phishing campaign.

	• Fifteen (15) email addresses of current employees and three (3) inactive email addresses of previous employees were targeted. Of the eighteen (18) targeted recipients, four (4) emails evaded the Organization's spam filter. • One (1) employee clicked on the link embedded in the email, which allowed the attacker to access the employee's email profile. • The unauthorized access resulted in a number of emails being forwarded to an unknown external email address, which contained the personal information of four (4) individuals. • On April 20, 2020, the Organization's IT Security team detected the activity, commenced an investigation, and contained and remediated the threat.
Affected individuals	The incident affected four (4) residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Undertook a programmatic and manual review of the email account to identity potential affected individuals. • Provided information pamphlets about the risks and warning signs of phishing campaigns to employees. • Provided access to complimentary credit monitoring and information pamphlet. • Increasing privacy training and resources around phishing awareness and reporting. • Enhanced IT Security protocols. • Enhanced security awareness training. • Engaged a third party specialist to validate remediation steps and review additional opportunities for security best practices.
Steps taken to notify individuals of the incident	Affected individuals were notified by telephone and letter on May 1, 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 reported: *Given the combination of personal information identifiers breached, there is a limited risk of fraud and identity theft. The combination of personal information, context of a relationship with [the Organization], and an email address could be used for phishing purposes.* In my view, a reasonable person would consider that the combination of contact information at issue, along with the individual's account number could be used to cause the significant harms of identity theft and fraud. Email address could be used for phishing, increasing 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, *There is a real risk harm could result from this incident given that the unauthorized access was the result of a phishing campaign with malicious intent. [The Organization] took steps to address the risk and substantially decrease the likelihood that harms will result, including: containing the incident within a reasonable amount of time; informing the individuals as soon as possible that their information was accessed in this incident; and providing affected individuals with credit monitoring and an educational pamphlet on phishing campaigns.* 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, the personal information may have been exposed for approximately 3 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 the combination of contact information at issue, along with the individual's account number could be used to cause the significant harms of identity theft and fraud. Email address could be used for phishing, increasing vulnerability to identity theft and fraud.

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, the personal information may have been exposed for approximately 3 weeks.

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 letter on May 1, 2020. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner