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-176 (File #016275)
Date notice received by OIPC	June 24, 2020
Date Organization last provided information	June 24, 2020
Date of decision	December 3, 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, • email address, • address, • telephone number, • signature, • social insurance number, • employment disciplinary letter, • conditions of employment, and • diagnostic health information. 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 May 4, 2020, an employee was subject to a targeted phishing attack. A malicious email directed the user to a webpage where they were prompted to enter their login credentials. • The attackers were able to use the credentials to access the employee's email account containing the information at issue. • The breach was discovered and contained 2 days later on May 6, 2020 by the Organization's IT Security team. • The Organization was unable to confirm whether the contents of the email were accessed.
Affected individuals	The incident affected 35 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Engaged external legal counsel. • Reviewed the email account to identify affected records. • Provided information pamphlets on phishing to affected individuals. • Provided company-wide notification about the risks associated with phishing and reminders to be vigilant. • Offered credit monitoring services to affected individuals. • Increased privacy training and resources available to employees. • Educated affected employee on cybersecurity best practices. • Removed option of using SINs on credit application forms. • Reviewed document and email management processes as related to the customer relationship management platform. • Initiated meeting to provide the affected group with tips for safely sharing information through email. • Reset impacted user's account password. • Removed all instances of the malicious email from systems. • Added additional monitoring controls. • Notified the Canadian Electricity Association, the Canadian Centre for Cyber Security, and law enforcement.
Steps taken to notify individuals of the incident	Affected individuals were notified by couriered mail, email, or telephone between May 22 and June 16, 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 "The primary harms that could result from this incident are those related to fraud, financial loss and identity theft. It is also possible that the combination of the personal information at issue and the affected individual's relationship with [the Organization] could lead to future phishing attempts, reputational damage and/or embarrassment." I agree with the Organization's assessment. A reasonable person would consider that the contact and identity information could be

	used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. Medical and employment information could be used to cause hurt, humiliation and embarrassment. 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 that "...there is a fair likelihood that harm may result from the incident". Further... *…the fact that the personal information at issue in the incident was potentially accessed by an unknown third party following a targeted phishing attempt suggests that there was a malicious intent involved in these circumstances. Additionally, some of the personal information at issue is considered to be particularly sensitive (such as SINs).* *On the other hand, the incident was identified and contained quickly, and much of the personal information that was potentially accessed is not particularly sensitive. Additionally, the individuals who were potentially affected have already received notice of the incident. [The Organization] has also provided such individuals with access to educational materials on phishing campaigns and free credit monitoring services to lessen the likelihood that harm will result from this incident.* In my view, 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). Further, the information may have been exposed for 2 days.

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 and identity information could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. Medical and employment information could be used to cause hurt, humiliation and embarrassment. 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). Further, the information may have been exposed for 2 days.

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 couriered mail, email, or telephone between May 22 and June 16, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner