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	SE Canada Inc. (Organization)
Decision number (file number)	P2021-ND-228 (File #019354)
Date notice received by OIPC	February 8, 2021
Date Organization last provided information	February 8, 2021
Date of decision	November 12, 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, • address, • telephone number (may include cell phone numbers), and • equipment type. 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 November 11, 2020, the Organization discovered that it was the victim of a ransomware attack by an unauthorized third party.

	• Based on its investigation, the Organization determined that the unauthorized user possibly had access to its systems as early as October 9, 2020. • The Organization reported that there is no indication that the data has been used or misused.
Affected individuals	The incident affected 225,176 individuals including 56,718 individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Disconnected systems, investigated, and engaged a cybersecurity firm to determine how the security incident occurred and the scope of such incident. • Reviewed cybersecurity and security measures. • Installed and implemented additional security measures and protocols. • Notified data protection regulators. • Encouraged individuals to be vigilant and provided tips and recourses for protecting the individual's identity.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on January 29, 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, *As telephone numbers were compromised and [the Organization] does not know whether such compromised telephone numbers included mobile telephone numbers, it is [the Organization's] assessment that there is a potential risk of phishing for the individuals affected through scams.* *The specified harm noted above, assuming they occur, could be significant as they can result in various telephone scams including fraud and ransom scams.* I accept the Organization's assessment. A reasonable person would consider the contact information, along with a cell phone number, could be used for 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	The Organization reported that it … *… is of the view that the likelihood that harm could result is low to moderate. While there is no evidence that the personal information at issue has been misused by the external actor, the personal information involved in the incident is not sensitive but could be used for the purposes of phishing. The fact that the*

between the incident and the possible harm.	*incident was caused as a result of the actions of an unknown actor with malicious intent additionally increases the likelihood that harm could result.* In my view, a reasonable person would consider 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, ransom demand). The lack of reported incidents resulting from this breach to date is not a mitigating factor, as phishing can occur months and even years after a data breach. As well, the personal information at issue may have been accessible for approximately one (1) month.

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 the contact information, along with a cell phone number, could be used for 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, ransom demand). The lack of reported incidents resulting from this breach to date is not a mitigating factor, as phishing can occur months and even years after a data breach. As well, the personal information at issue may have been accessible for approximately one (1) month.

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 January 29, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner