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	E.H. Wachs (Organization)
Decision number (file number)	P2020-ND-153 (File #015943)
Date notice received by OIPC	May 27, 2020
Date Organization last provided information	November 16, 2020
Date of decision	November 20, 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 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 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, and • social insurance number. 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	• The Organization discovered that, from February 15 to February 28, 2020, unauthorized individuals installed ransomware on certain of its servers.

	• The Organization reported that although unauthorized individuals could have infiltrated the servers, it had no reason to believe that any personal information was viewed or accessed.
Affected individuals	The incident affected 16 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Launched an internal investigation. • Reviewed security controls. • Retained a forensic security firm to assist and evaluate systems and processes to further strengthen protections for its servers. • Provided notification to affected individuals. • Provided credit monitoring services for two years.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on May 15, 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 that it "…recognizes that, in light of the personal information that could have potentially been available to the perpetrator(s) of this unauthorized access, there is a possibility of harm to the affected individuals in the form of identity theft...". In my view, a reasonable person would consider the contact and identity information at issue could be used to cause the significant harms of 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 it "…has not discovered any information to make it believe that any personal information in fact was actually accessed or viewed or has been misused in any way...". 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, ransomware). Although the Organization said it "has not discovered any information to make it believe that any personal information in fact was actually accessed or viewed or has been misused in any way ", the Organization also reported that the information "could have potentially been available to the perpetrator(s)". Further, the personal information may have been available to the perpetrators for two (2) 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 the contact and identity information at issue could be used to cause the significant harms of 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 (deliberate intrusion, ransomware). Although the Organization said it "has not discovered any information to make it believe that any personal information in fact was actually accessed or viewed or has been misused in any way ", the Organization also reported that the information "could have potentially been available to the perpetrator(s)". Further, the personal information may have been available to the perpetrators for two (2) 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 May 15, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner