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	Millennium EMS Solutions Ltd. (Organization)
Decision number (file number)	P2018-ND-108 (File #003953)
Date notice received by OIPC	September 30, 2016
Date Organization last provided information	July 20, 2018
Date of decision	August 9, 2018
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 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)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The following information was involved in this incident: • name, • address, • telephone number, • date of birth, and • social insurance number. 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 September 1, 2016, the Organization's IT Helpdesk received reports of a malfunctioning IT server system. After investigation, it was determined that the system "had been hacked by external hackers on July 5, 2016".

	• The unauthorized access to the server was through a default user account in the system. • Unauthorized software was downloaded that was not compatible with the system.
Affected individuals	The incident affected 330 residents of Alberta, including 230 former employees and 100 active employees or contract vendors.
Steps taken to reduce risk of harm to individuals	• All related services were immediately disabled and a system log started. • Remote access to the server and all network systems disabled. Systems with remote access enabled were inspected for possible unauthorized access. • Server inspected for malicious software and rootkits. • Police notified on September 2, 2016. • On September 4, 2016 external Cyber Specialists were retained. • New intrusion detection system was implemented. • New/enhanced authentication procedure was implemented. • System password and local administrator account password reset. • System reconfiguration. • Removal of SIN and date of birth from the system.
Steps taken to notify individuals of the incident	The Organization notified employees by email on September 3, 6 and 18, 2016. Notification to former employees occurred for those that the Organization was able to trace. On September 8, 2016, a town hall meeting took place at all office locations (Edmonton, Calgary and Grande Prairie) with audio conferencing for individuals not in the offices. On September 19, 2016 an update was provided during an Operations meeting to all staff. This meeting took place at all office locations (Edmonton, Calgary and Grande Prairie) with audio conferencing for individuals not in the offices.
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 "Access to information on individual's name, SIN and Date of Birth could result in identity theft." I agree with the Organization. The 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 "…internal IT professionals and external experts retained to fully investigate the issue did not identify any transfer of information from our server, therefore the assessment is that the unauthorized access does not represent a real risk of significant harm. Based on our assessment the likelihood of harm is low." Further, "To date there is no evidence that sensitive personal information was accessed or the exfiltration of such data. Multiple searches on all endpoints to identify compromises, anomalies, malware, vulnerabilities and other conditions that would expose a threat have come back with no indication of the presence of a malicious actor". 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 (deliberate unauthorized intrusion). Further the information may have been exposed for approximately 2 months. Although the Organization said that "To date there is no evidence that sensitive personal information was accessed or the exfiltration of such data", I do not have enough information to reassure me that the perpetrators could not or did not access or exfiltrate personal information, particularly considering the Organization *also* reported that "the access was used for web related activities such as: multiple banking, virtual currency and social media sites."

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 in this case.

The identity information at issue could be used to cause the significant harms of identity theft and fraud. 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 (deliberate unauthorized intrusion). Further the information may have been exposed for approximately 2 months.

Although the Organization said that "To date there is no evidence that sensitive personal information was accessed or the exfiltration of such data", I do not have enough information to reassure me that the perpetrators could not or did not access or exfiltrate personal information, particularly considering the Organization *also* reported that "the access was used for web related activities such as: multiple banking, virtual currency and social media sites."

The Organization is required to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified current employees by email and through meetings on September 3, 6, 8, 18 and 19, 2016. The Organization notified former employees whom they had contact information for. The Organization reported that the notifications met the requirements of section 19.1 of the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner