



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Society for Industrial and Applied Mathematics (Organization)
Decision number (file number)	P2017-ND-82 (File #003637)
Date notice received by OIPC	August 12, 2016
Date Organization last provided information	August 12, 2016
Date of decision	June 19, 2017
Summary of decision	There is a real risk of significant harm to the individual affected by this incident. The Organization is required to notify the individual pursuant to section 37.1 of the <i>Personal Information Protection Act</i> (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA “organization”	The Organization operates on a not for profit basis; however, it is not a “non-profit organization” as defined in section 56(1)(b) of PIPA. The Organization is an “organization” as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA “personal information”	<p>The incident involved the following information:</p> <ul style="list-style-type: none">• name,• address,• telephone number,• email address, and• credit card information. <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA. Some of the information concerns a resident of Alberta.</p>
DESCRIPTION OF INCIDENT	
<input checked="" type="checkbox"/> loss <input type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	

Description of incident	<ul style="list-style-type: none"> On or about June 20, 2016 the Organization learned that personal information of a member that was stored on the computer system of a vendor may have been compromised. The vendor advised the Organization that its computer system was affected by ransomware/malware and an unauthorized user gained access to data on the computer system.
Affected individuals	The incident affected one (1) resident of Alberta.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> Took steps to eliminate any unauthorized access. The vendor reported the matter to law enforcement. Terminated relationship with the vendor. Providing 1 year of free credit monitoring to the affected individual in Alberta.
Steps taken to notify individuals of the incident	The affected individual in Alberta was notified of the incident by letter on August 2, 2016.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
<p>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.</p>	<p>The Organization reported “The intruder was engaging in ransomware activities and there is no indication that the credit card information of the single Alberta resident was acquired or used. Generally speaking, exposure of credit card information could possibly result in fraudulent charges and/or identity theft.”</p> <p>In my view, the financial information involved in this incident could be used to cause the harms of identity theft, fraud and financial loss. In addition, the email address could be used for phishing purposes. These are significant harms.</p>
<p>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.</p>	<p>The Organization reported “The intruder was engaging in ransomware activities and there is no indication that the credit card information of the single Alberta resident was acquired or used. Under these circumstances, it appears that the risk of harm is low.”</p> <p>In my view, there is a real risk of harm resulting from this incident. The incident was the result of malicious intent (deliberate unauthorized access) and the Organization cannot confirm that information was not acquired or accessed.</p>

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 individual. The financial information involved in this incident could be used to cause the harms of identity theft, fraud and financial loss. The email address could be used for phishing purposes. These are significant harms. The incident was the result of malicious intent (deliberate unauthorized access) and the Organization cannot confirm that information was not acquired or accessed.

I require the Organization to notify the affected individual in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the affected individual in Alberta was notified of the incident by letter on August 2, 2016. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner