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	Health Standards Organization (HSO) and Accreditation Canada (AC) (Organization)
Decision number (file number)	P2020-ND-018 (File #013700)
Date notice received by OIPC	September 11, 2019
Date Organization last provided information	September 13, 2019
Date of decision	February 13, 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 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 a registered non-profit standards development organization headquartered in Ontario and is an “organization” as defined in section 1(1)(i) of PIPA. The Organization is not a “non-profit organization” as defined in PIPA, such that PIPA would only apply to personal information collected, used or disclosed in connection with a commercial activity.
Section 1(1)(k) of PIPA “personal information”	The Organization reported: *The forensic investigation team found no evidence that any personal information has actually been affected by the ransomware in issue. However, the types of personal information that was stored on the affected servers may include the following: name, address, email address, social insurance and banking information of individual … staff, surveyors, Technical Committee members, Board Members and third party contractors.* This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA. To the extent this information was collected in Alberta, PIPA applies.

<table>
<tr><th colspan="2">DESCRIPTION OF INCIDENT</th></tr>
<tr><td colspan="2">☒ loss ❑ unauthorized access ❑ unauthorized disclosure</td></tr>
<tr><td><b>Description of incident</b></td><td>• On June 21, 2019, the Organization became aware of a potential malware incident which impacted its IT systems. The incident was later determined to have been caused by the "Ryuk" ransomware that encrypts all data on the infected servers rendering it inaccessible/unreadable until a ransom is paid.
• The Organization’s investigation did not find any evidence of any information disclosure resulting from the incident, which is consistent with the fact that the Ryuk ransomware is not known to exfiltrate information prior to encrypting the files on infected servers.</td></tr>
<tr><td><b>Affected individuals</b></td><td>The incident affected 1,246 individuals, including 66 in Alberta.</td></tr>
<tr><td><b>Steps taken to reduce risk of harm to individuals</b></td><td>• Retained a third party IT forensic investigation team specializing in cybersecurity.
• Took robust measures to promptly contain the breach, mitigate its effects and prevent future recurrence of the incident.</td></tr>
<tr><td><b>Steps taken to notify individuals of the incident</b></td><td>Affected individuals in Alberta were notified by email by September 11, 2019.</td></tr>
<tr><th colspan="2">REAL RISK OF SIGNIFICANT HARM ANALYSIS</th></tr>
<tr><td><b>Harm</b>
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.</td><td>The Organization reported “Possible harm that may result from misuse of financial information may include fraud, identity theft, or exposure to phishing campaigns or attempts to obtain further personal information”.
I accept the Organization’s assessment that the contact and financial information at issue could be used to cause the harms of fraud and identity theft. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms.</td></tr>
<tr><td><b>Real Risk</b>
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.</td><td>The Organization reported “At this time, we assess the likelihood that harm will result as moderate” based, in part, on the following:
• “The ransomware attack appear to have been perpetrated by hackers looking to profit from the attack. On the other hand, the forensic investigation team advised that the specific "Ryuk" ransomware in issue has relatively low technical capabilities, as it functions to encrypt the files to hold them for</td></tr>
</table>

	ransom and is not known to exfiltrate information prior to encrypting the infected files”. • “The forensic investigation team found no evidence that any personal information has actually been compromised in any way. However, the possibility that unauthorized access may have occurred cannot be ruled out”. In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the incident appears to be the result of malicious action (ransomware). Although the Organization reported the specific ransomware at issue is “not known to exfiltrate information”, the Organization also reported that “…unauthorized access may have occurred cannot be ruled out”.

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 individuasl.

The contact and financial information at issue could be used to cause the harms of fraud and identity theft. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms. The likelihood of harm resulting from this incident is increased because it appears to be the result of malicious action (ransomware). Although the Organization reported the specific ransomware at issue is “not known to exfiltrate information”, the Organization also reported that “…unauthorized access may have occurred cannot be ruled out”.

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 that affected individuals in Alberta were notified by email by September 11, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner