



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	The Helicopter Association of Canada (Organization)
Decision number (file number)	P2019-ND-109 (File #011558)
Date notice received by OIPC	January 10, 2019
Date Organization last provided information	January 10, 2019
Date of decision	July 19, 2019
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. Pursuant to section 37.1 of the <i>Personal Information Protection Act</i> (PIPA), the Organization is required to notify those individuals whose personal information was collected in Alberta.
JURISDICTION	
Section 1(1)(i) of PIPA “organization”	The Organization is an Ontario based non-profit organization that services the Canadian helicopter industry; however, it is not a “non-profit organization” as defined in PIPA, such that PIPA only applies to personal information collected, used or disclosed in connection with a commercial activity. Instead, 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">• first and last name,• mailing address,• email address,• telephone number,• banking information, credit card information and invoices (in some cases). <p>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.</p>
DESCRIPTION OF INCIDENT	
<input type="checkbox"/> loss <input checked="" type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	

<p>Description of incident</p>	<ul style="list-style-type: none"> • On September 18, 2018, an unidentified party gained access to an employee’s email account. • The unidentified party applied a forwarding rule and copied the contents of the employee’s email account. The cause of the incident is a phishing email containing a malicious link that was received by the employee. • The breach was discovered on October 11, 2018, when the employee sent an internal email to her assistant and received a bounce back message stating that the email inbox full. • The unidentified party’s access was terminated immediately upon discovery on October 11, 2018.
<p>Affected individuals</p>	<p>The incident affected approximately 4,800 people, including 48 individuals who were or potentially are residents of Alberta.</p>
<p>Steps taken to reduce risk of harm to individuals</p>	<ul style="list-style-type: none"> • Turned off the email forwarding rule. • Changed the password for the email account. • Enabled multi-factor authentication for all email accounts, • Enabled email archiving, auditing and antivirus scanning. • Will install additional security features for its network. • Will offer a call centre with access to a fraud specialist to answer questions arising.
<p>Steps taken to notify individuals of the incident</p>	<p>Affected individuals were notified by email beginning October 15, 2018 and through to January 9, 2019.</p>
<p>REAL RISK OF SIGNIFICANT HARM ANALYSIS</p>	
<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 that “Based on the information that was accessed, there is a risk of phishing, identity theft and fraud.”</p> <p>I agree with the Organization’s assessment. A reasonable person would consider that the contact and financial information at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud.</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 “It is possible that the unauthorized party may use the personal information to harm affected individuals in the form of identity theft or fraud...the unauthorized party exfiltrated the contents of the email account and has access to the emails and attachments.”</p> <p>In my view, a reasonable person would consider that the likelihood of harm resulting in this case is increased because the breach</p>

	resulted from malicious intent (unauthorized access) and the information was exfiltrated.
DECISION UNDER SECTION 37.1(1) OF PIPA	
<p>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.</p> <p>A reasonable person would consider that the contact and financial information at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. The likelihood of harm resulting in this case is increased because the breach resulted from malicious intent (unauthorized access) and the information was exfiltrated.</p> <p>I require the Organization to notify the affected individuals whose personal information was collected in Alberta, in accordance with section 19.1 of the <i>Personal Information Protection Act Regulation</i> (Regulation).</p> <p>I understand that Affected individuals were notified by email beginning October 15, 2018 and through to January 9, 2019. The Organization is not required to notify affected individuals again.</p>	

Jill Clayton
Information and Privacy Commissioner