



**PERSONAL INFORMATION PROTECTION ACT**  
**Breach Notification Decision**

<b>Organization providing notice under section 34.1 of PIPA</b>	StorageVault Canada Inc. dba Access Storage (Organization)
<b>Decision number (file number)</b>	P2020-ND-127 (File# 013757)
<b>Date notice received by OIPC</b>	October 24, 2019
<b>Date Organization last provided information</b>	October 24, 2019
<b>Date of decision</b>	October 27, 2020
<b>Summary of decision</b>	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify the individual whose personal information was collected in Alberta pursuant to section 37.1 of the <i>Personal Information Protection Act</i> (PIPA).
<b>JURISDICTION</b>	
<b>Section 1(1)(i) of PIPA “organization”</b>	The Organization is based in Scarborough, Ontario, and has storage facilities throughout Canada. The Organization is an “organization” as defined in section 1(1)(i) of PIPA.
<b>Section 1(1)(k) of PIPA “personal information”</b>	<p>The incident involved all or some of the following information:</p> <ul style="list-style-type: none"><li>• name,</li><li>• address,</li><li>• telephone number,</li><li>• email address,</li><li>• date of birth,</li><li>• driver's license information,</li><li>• financial information provided at the time of the rental, either banking information or a credit card number,</li><li>• secondary ID provided at the time of the rental, for example a passport, birth certificate, social security card, etc.</li></ul> <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>
<b>DESCRIPTION OF INCIDENT</b>	
<input checked="" type="checkbox"/> loss <input type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	

<p><b>Description of incident</b></p>	<ul style="list-style-type: none"> <li>On September 16, 2019, the Organization learned that it was the victim of a break and enter, which occurred on September 15, 2019 at its facility in Winnipeg, Manitoba.</li> <li>The perpetrators broke into a locked storage unit which contained the Organization’s records, including physical files with client personal information collected for the purposes of facilitating storage rentals and services.</li> <li>The Organization reported the break-in to police, who were able to apprehend one of the thieves and recover a portion of the records, including 79 of the 225 client files stolen.</li> </ul>
<p><b>Affected individuals</b></p>	<p>A total of 225 individuals were affected, including 1 Alberta resident.</p>
<p><b>Steps taken to reduce risk of harm to individuals</b></p>	<ul style="list-style-type: none"> <li>Reported break-in to law enforcement and working with police as the investigation is ongoing.</li> <li>Conducted an internal investigation to identify affected clients and the personal information at issue.</li> <li>Upgrading locks on storage units.</li> <li>Reviewing privacy policy and re-assessing the information collected for client services in order to make revisions where appropriate.</li> <li>Implementing employee training and reviewing safeguards to protect client information.</li> <li>Implementing regular audits of safeguards relating to the collection, storage, and protection of client information.</li> <li>Provided affected individuals with complimentary one year credit and identity theft monitoring services.</li> </ul>
<p><b>Steps taken to notify individuals of the incident</b></p>	<p>Affected individuals were notified by email and mail on October 8 and October 9, 2019.</p>
<p><b>REAL RISK OF SIGNIFICANT HARM ANALYSIS</b></p>	
<p><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.</p>	<p>The Organization reported that although it “...is not aware of the reason or motive for the break-in, [the Organization] was advised [sic] by the Winnipeg Police that the theft was possibly targetted for the purposes of identity theft. In addition, there is a risk of financial fraud and phishing based on the personal information contained in Access Storage’s client files.”</p> <p>In my view, a reasonable person would consider the contact, identity, and financial information at issue could be used to cause the harms of identity theft and fraud. Email address could be used for phishing, increasing vulnerability to identity theft and fraud.</p>

<p><b>Real Risk</b></p> <p>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 “There is a real risk of significant harm to affected individuals of financial fraud, identity theft, and phishing based on the categories of personal information potentially contained in [the] client files.”</p> <p>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 malicious action (break-in and theft). Not all of the information was recovered.</p>
<p><b>DECISION UNDER SECTION 37.1(1) OF PIPA</b></p>	
<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 the contact, identity, and financial information at issue could be used to cause the harms of identity theft and fraud. Email address could be used for phishing, increasing vulnerability to identity theft and fraud. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to malicious action (break-in and theft). Not all of the information was recovered.</p> <p>I require the Organization to notify the affected individual whose personal information was collected in Alberta, in accordance with section 19.1 of the <i>Personal Information Protection Act Regulation</i>. I understand the Organization notified the affected individuals by email and mail on October 8 and October 9, 2019. The Organization is not required to notify the affected individual again.</p>	

Jill Clayton  
Information and Privacy Commissioner