



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	2002358 Alberta Ltd. o/a The Captains Boil (Organization)
Decision number (file number)	P2019-ND-011 (File #010475)
Date notice received by OIPC	November 7, 2018
Date Organization last provided information	November 7, 2018
Date of decision	February 4, 2019
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 pursuant to section 37.1 of the <i>Personal Information Protection Act</i> (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA “organization”	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,• date of birth, and• social insurance number. <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA.</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">• A personal/work truck was broken into during the early morning hours of October 28, 2018, outside of a residential home.• The truck contained some documents in a briefcase that may have contained personal information of employees of the Organization, and also contained a secured iPad with personal information.

	<ul style="list-style-type: none"> • The Organization reported that “The majority of information possibly accessed was contained on a secured iPad, with a 6 digit passcode, which was not written down.” • The break-in was discovered the same day.
Affected individuals	The incident affected 39 individuals.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> • Reported the breach to law enforcement. • In the future, no documents or electronic files containing personal information will be left in any vehicle or unsecured location. • All iPads, tablets, and other electronic file sources which may allow an unauthorized individual to access personal information will be secured with a passcode, and, to the extent possible, any features that allow the owner of the device to erase the device remotely will be engaged so that the device may be erased in the event of a theft.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter and email November 7, 2018
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
<p>Harm</p> <p>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 possible harms that may occur as a result of the breach include “Identity theft.”</p> <p>In my view, the identity and contact information at issue could be used to cause the significant harms of identity theft and fraud.</p>
<p>Real Risk</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 “The iPad, which contained the most personal information, was secured with a six digit passcode, so the risk is likely minimal. The physical [sic], paper documents contained in the truck that may have been taken could have contained similar information, so there is some risk.”</p> <p>In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the incident resulted from malicious intent (theft). It is not clear to me from the Organization’s report if the iPad was encrypted. To the extent it was not encrypted, personal information on the iPad could potentially be accessed. Further, the Organization did not report recovering the information.</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 individuals.

The identity and contact 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 incident resulted from malicious intent (theft). It is not clear to me from the Organization's report if the iPad was encrypted. To the extent it was not encrypted, personal information on the iPad could potentially be accessed. Further, the Organization did not report recovering the information.

I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation), including any individuals whose personal information was stored on the iPad, if the iPad was not encrypted.

I understand the Organization reported that affected individuals were notified by letter and email on November 7, 2018. If this includes individuals whose personal information was on the iPad (and if the iPad was not encrypted), then the Organization is not required to notify affected individuals again. **Otherwise, the Organization is required to confirm to my office in writing within 10 days of the date of this decision that all affected individuals have been notified in accordance with the Regulation.**

Jill Clayton
Information and Privacy Commissioner