



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	1219146 Alberta Ltd. (Organization)
Decision number (file number)	P2021-ND-302 (File #017453)
Date notice received by OIPC	April 9, 2020
Date Organization last provided information	April 9, 2020
Date of decision	March 3, 2022
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify those 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 operates in Alberta and 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 contents of a safe, which contained some or all of the following human resource-type information:</p> <ul style="list-style-type: none">• name,• home address,• social insurance number,• bank account information, and• deposit details. <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">• Between March 27, 2020 and March 28, 2020, the Organization’s office was broken into and the Organization’s safe was stolen and subsequently compromised.• The safe contained unencrypted external hard drives used to back-up data from individually assigned computers.

Affected individuals	The incident affected 20 individuals.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> • Recommended that affected individuals take steps to mitigate risk (e.g. change relevant passwords, register with Equifax or TransUnion, be vigilant for fraudulent activity in accounts). • Enhanced security of premises. • Reported the incident to the local police service.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on April 6, 2020.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
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.	The Organization reported the possible harm that may occur as a result of the breach are “Losses related to identity theft.” In my view, a reasonable person would consider that the contact, identity and financial information at issue could be used to cause the significant harms of identity theft, and fraud.
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.	The Organization reported there is “No evidence of harm to date. Four attempted uses of information known to date, none involving company staff.” In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased as it was the result of malicious intent (break-in and theft). As well, there was four attempted uses of information known to date. The lack of actual harms resulting to date is not a mitigating factor, as identity theft and fraud can occur months and even years after a data breach.
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. A reasonable person would consider that the contact, identity and financial information at issue could be used to cause the significant harms of identity theft, and fraud. The likelihood of harm resulting from this incident is increased as it was the result of malicious intent (break-in and theft). As well, there was four attempted uses of information known to date. The lack of actual harms resulting to date is not a mitigating factor, as identity theft and fraud can occur months and even years after a data breach. I require the Organization to notify the affected individuals in Alberta in accordance with section 19.1 of the <i>Personal Information Protection Act Regulation</i> (Regulation).	

I understand the Organization notified affected individuals in an email dated April 6, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner