



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	FPI Management (Organization)
Decision number (file number)	P2021-ND-295 (File #020706)
Date notice received by OIPC	April 16, 2021
Date Organization last provided information	April 16, 2021
Date of decision	March 2, 2022
Summary of decision	There is a real risk of significant harm to the individual 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).
JURISDICTION	
Section 1(1)(i) of PIPA “organization”	The Organization is a property management company, headquartered in Folsom, California, USA, 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 all or some of the following information:</p> <ul style="list-style-type: none">• name,• address, and• social security number. <p>This information is about an identifiable individual 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	
Description of incident	<ul style="list-style-type: none">• On August 14, 2020, the Organization learned that it experienced a data security incident that disrupted access to certain of its systems.• An unauthorized third party gained access to certain of the Organization’s systems and personal information stored on these systems was accessed or acquired without authorization.

	<ul style="list-style-type: none"> On March 3, 2021, the Organization determined that personal information belonging to one Alberta resident may have been accessed or acquired without authorization.
Affected individuals	The incident affected one (1) individual whose personal information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> Took immediate steps to secure systems prior to restoration. Engaged legal counsel to guide an external investigation, and retained independent cybersecurity experts to investigate. Offered the affected individual complimentary identity theft restoration and credit monitoring services.
Steps taken to notify individuals of the incident	The affected individual was notified by letter on April 16, 2021.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
<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 did not specifically identify any harms that might result from this incident, but its notification to the affected individual stated...</p> <p><i>...we recommend that you remain vigilant and review your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company that maintains your account. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities.</i></p> <p>In my view, a reasonable person would consider that the contact and identity information at issue could be used to cause the significant harms of 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 did not specifically provide an assessment of the likelihood that significant harm would result from this incident, but its notification to affected individuals stated that it “... is not aware of the misuse of any potentially impacted information in connection with this incident”.</p> <p>In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased because it resulted from the malicious action of an unknown third party (deliberate intrusion). The lack of reported incidents to date is not a mitigating factor, as fraud or financial loss can happen months and even years after a data breach.</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 individual.

A reasonable person would consider that the contact and identity 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 because it resulted from the malicious action of an unknown third party (deliberate intrusion). The lack of reported incidents to date is not a mitigating factor, as fraud or financial loss can happen months and even years after a data breach.

I require the Organization to notify the affected individual whose personal information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified the affected individual by letter on April 16, 2021. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner