



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Cornerstone Building Brands (Organization)
Decision number (file number)	P2022-ND-072 (File #023165)
Date notice received by OIPC	September 3, 2021
Date Organization last provided information	September 3, 2021
Date of decision	January 9, 2023
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 an “organization” as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA “personal information”	<p>The incident involved some or all of the following information:</p> <ul style="list-style-type: none">• name, and• Social Insurance Number. <p>This information is about identifiable individual and is “personal information” as defined in section 1(1)(k) of PIPA. To the extent the information at issue 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 November 30, 2020, the Organization experienced a data security incident.• The Organization’s investigation found unauthorized access to a limited number of systems in its network.• The Organization also learned that an unauthorized person had accessed certain information that was stored on its systems in late December 2020.

	<ul style="list-style-type: none"> A comprehensive review of the files was conducted and determined that they contained information pertaining to one Alberta resident.
Affected individuals	The incident affected 2659 individuals, including 1 individual whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	<p>Steps taken by the Organization includes, but are not limited to:</p> <ul style="list-style-type: none"> Took steps to further secure the network. Notified law enforcement. Launched an investigation with a leading forensics firm. Offered complimentary, one-year membership for credit monitoring and identity theft prevention. Recommended that the individual closely review their financial statements for any unauthorized activity. Implementing additional safeguards and technical security measures.
Steps taken to notify individuals of the incident	The affected individual was notified by letter on September 3, 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 reported,</p> <p style="text-align: center;"><i>Stolen Social Insurance numbers can be used to commit identity theft.</i></p> <p>In my view, a reasonable person would consider that the identity information at issue could be used to cause the harms of identity theft, fraud or financial loss. These are all significant harms.</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,</p> <p style="text-align: center;"><i>CBB is offering the Alberta resident a complimentary, one-year membership to TransUnion credit monitoring and identity theft prevention. To further diminish the likelihood of harm, CBB is recommending that the individual closely review their financial statements for any unauthorized activity.</i></p> <p>In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). Although the Organization has adopted additional safeguards, these were not in place at the time of the breach. Further, this does not necessarily</p>
--	--

	mitigate the potential harm that may result if the information accessed from the Organization’s systems were to be used for fraudulent purposes. Finally, the information at issue was exposed for approximately three (3) weeks.
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 individual.</p> <p>The identity information at issue could be used to cause the harms of identity theft, fraud or financial loss. These are all significant harms.</p> <p>The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). Although the Organization has adopted additional safeguards, these were not in place at the time of the breach. Further, this does not necessarily mitigate the potential harm that may result if the information accessed from the Organization’s systems were to be used for fraudulent purposes. Finally, the information at issue was exposed for approximately three (3) weeks.</p> <p>I require the Organization to notify the affected individual whose 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 the Organization notified the affected individual by letter on September 3, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individual again.</p>	

Cara-Lynn Stelmack
Assistant Information and Privacy Commissioner