Office of the Information and
Privacy Commissioner of Alberta

PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Cornerstone Building Brands (Organization)
Decision number (file number)	P2021-ND-169 File #018302)
Date notice received by OIPC	November 20, 2020
Date Organization last provided information	November 20, 2020
Date of decision	August 26, 2021
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 whose personal information was collected in Alberta, pursuant to section 37.1 of the *Personal Information Protection Act* (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"	The incident involved all or some of the following information: • name, • date of birth, • driver's license number, and/or • financial account information. 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.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On August 3, 2020, the Organization discovered unusual network activity. • The Organization's investigation determined that an unauthorized party gained access to the network between August 3, 2020 and August 9, 2020. • The Organization conducted a comprehensive review of all files involved, and determined on October 22, 2020, that they contained personal information. • The unauthorized party acquired copies of certain information pertaining to a limited number of individuals that was stored within the Organization's systems. • The Organization reported that it had no evidence that any information has or will be used, and that it arranged for the unauthorized party to delete the files that were removed from the network. The Organization does not believe there was any public disclosure of the files or information contained therein.
Affected individuals	The incident affected 47 individuals, of which 25 individuals had their information collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Notified law enforcement. • Investigated and engaged third-party specialists to assist. • Offered eligible individuals a complimentary, one-year membership to credit monitoring and identity theft protection service. • Recommended that affected individuals closely review their financial and/or medical statements for any unauthorized activity. • Established a dedicated call center. • Implementing further network monitoring tools and further strengthened its security processes.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on November 20, 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 that "Drivers' license numbers can be used to potentially commit identity theft." In my view, a reasonable person would consider 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 that it... *… has no evidence that any information has or will be used. [The Organization] also arranged for the unauthorized party to delete the files that were removed from the network and does not believe there was any public disclosure of the files or information contained therein."* 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) and personal information was accessed and stolen. The lack of reported incidents of identity theft or fraud to date is not a mitigating factor as identity theft and fraud can happen months and even years after a data breach. Although the Organization reported the unauthorized party deleted the files, it is not clear how reliable this information may be. Finally, the personal information was in the cybercriminal's possession for approximately 6 weeks.

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 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 because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion) and personal information was accessed and stolen. The lack of reported incidents of identity theft or fraud to date is not a mitigating factor as identity theft and fraud can happen months and even years after a data breach. Although the Organization reported the unauthorized party deleted the files, it is not clear how reliable this information may be. Finally, the personal information was in the cybercriminal's possession for approximately 6 weeks.

I require the Organization to notify the affected individuals 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 affected individuals by letter on November 20, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner