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	Forest City Trade Group, LLC and its affiliated companies (Organization)
Decision number (file number)	P2022-ND-019 (File #022467)
Date notice received by OIPC	July 27, 2021
Date Organization last provided information	July 27, 2021
Date of decision	April 22, 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 *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, • address, and • social insurance number. 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.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• On June 24, 2021, the Organization discovered anomalous security activity when a computer administrator's remote desktop session was interrupted. • The Organization determined it was the victim of a ransomware attack. Files and systems were encrypted. The attack began on June 21, 2021. • Simultaneous ransomware encryption attacks were then executed overnight against servers and workstations.

	• The attack may have resulted in the unauthorized access and acquisition of personal information.
Affected individuals	The incident affected 1855 individuals, including 1 individual whose personal information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Notified law enforcement. • Engaged a third-party cybersecurity expert. • Deployed enterprise-wide endpoint monitoring solutions to detect any continued presence of the threat actors in its systems. • Offered complimentary ID theft and credit monitoring services for two-years. • Working to identify how this incident occurred. • Will continue to assess its security practices and take steps, as necessary, to minimize the risk of a similar incident occurring in the future.
Steps taken to notify individuals of the incident	The affected individual was notified by letter on July 22, 2021.
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 the possible harms that may occur as a result of the breach are "Identity theft or fraud." I agree with the Organization's assessment. A reasonable person would consider the contact and identity 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, *Names and Social Insurance Numbers were potentially compromised by unknown individuals which could lead to identity theft or fraud.* In my view, a reasonable person would consider that 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, ransomware). Further, the information may have been available to the unauthorized third party for approximately 4 days.

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 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 the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion, ransomware). Further, the information may have been available to the unauthorized third party for approximately 4 days. 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 July 22, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance