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	Carey Management Inc. (Organization)
Decision number (file number)	P2022-ND-017 (File #022420)
Date notice received by OIPC	July 26, 2021
Date Organization last provided information	July 26, 2021
Date of decision	August 30, 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 Personal Information Protection Act (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is a holding company for several related entities and subsidiaries including Spruce It Up Garden Center Inc. Spruce It Up Garden Center Inc. is a full-service garden center located in Calgary, Alberta.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • photograph, • home address, • email address, • telephone number, • date of birth, • social insurance number, • driver's license information, • banking and other financial income and benefits information (including TD1 tax credit for, and/or T1 tax and benefit return form), and • emergency contact information. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On May 9, 2021, the Organization became aware that it was the subject of a cybersecurity incident, which resulted in the unauthorized access of some personal information of current and former employees of Spruce It Up Garden Center Inc. • The perpetrators of the cybersecurity incident used malicious software to circumvent security safeguards and were able to obtain unauthorized access to the Organization's systems. • The Organization engaged their third-party security operations center to help rapidly investigate and address this matter. Within 24 hours of the incident, the Organization was able to contain the breach and prevent any further unauthorized access.
Affected individuals	The incident affected approximately 248 individuals.
Steps taken to reduce risk of harm to individuals	• Provided affected individuals with 12 months of credit monitoring services without charge. • Executed its security incident response procedures and investigation activities. • Completed password resets for all system service accounts, performed a security review of its security monitoring software and implemented additional protection measures, performed additional automated and manual scans/reviews for vulnerabilities, and expanded its monitoring for threats. • Reported incident to law enforcement.
Steps taken to notify individuals of the incident	Affected individuals were notified by mail on July 13, 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.	In its letter to my office, the Organization did not provide an assessment of the likelihood of harm. However, the Organization's notification to affected individuals stated: *We also encourage you to consider the following:* *• Remain vigilant against threats of identity theft or fraud, and regularly review and monitor your account statements and credit history for any signs of unauthorized transactions or activity.* *• While we have no evidence that information accessed in this attack is being misused, if you ever suspect that you are*

	the victim of identity theft or fraud, or if you believe your information was used for fraudulent purposes, we strongly recommend you contact your local police department and the Canadian Anti-Fraud Centre at 1-888-495-8501, or by visiting: www.antifraudcentre-centreantifraude.ca *• As always, you should be alert for "phishing" emails or phone calls from someone who acts like they know you or are a company that you may do business with and requests sensitive information over email or the phone, such as passwords, Social Insurance Number, or bank account information.* In my view, a reasonable person would consider that the contact, identity, and financial information could be used to cause identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are significant harms.
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's notification to affected individuals stated: *At this time, we do not have any evidence that the affected personal information was used to commit fraud or otherwise misused. However, it is always a good idea to review your account information and update personal identification number (PIN/passcode) on your bank and other accounts.* 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). I do not believe that the lack of reported incidents of identity theft or fraud to date is a mitigating factor in the likelihood of harm resulting from this incident, as identity theft can happen months and even years after a data breach. Further, the information may have been exposed for 24 hours.

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.

The contact, identity, and financial information could be used to cause identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are significant harms.

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). I do not believe that the lack of reported incidents of identity theft or fraud to date is a mitigating factor in the

likelihood of harm resulting from this incident, as identity theft can happen months and even years after a data breach. Further, the information may have been exposed for 24 hours.

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 mail on July 13, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance