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	Carl's Golfland (Organization)
Decision number (file number)	P2020-ND-002 (File #013695)
Date notice received by OIPC	September 11, 2019
Date Organization last provided information	September 11, 2019
Date of decision	January 31, 2020
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify the 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 the following information: • first and last name, • address, • shipping information, • email address, • telephone number, and • credit card information (card number, expiration date, and CVV). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta via the Organization's ecommerce website mec.ca.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On March 25, 2019, a webshell was inserted into the Organization's website through a vulnerability and brute force attack. • Customers who made online purchases between the dates of March 25 through July 14, 2019 were affected. • The breach was discovered on July 14, 2019 as the result of a bank inquiry.
Affected individuals	The incident affected 24,772 individuals, including 14 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Reported incident to law enforcement. • Conducted multiple malware scans, forensic analysis of admin and access logs, backups and other artifacts of the system, isolated and removed malware scripts and files. • Deployed additional security monitoring and security tools.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on August 29, 2019.
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 "The risk is that the unauthorized individuals will use or sell credit card information." In my view, a reasonable person would consider that the contact and financial information at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to 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 there is "A siginificant [sic] risk of harm in that the unauthorized individuals could use the affected individuals credit card information to transact financial transactions". In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the incident resulted from malicious action (deliberate attack) and the breach was not discovered for almost 4 months.
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 that the contact and financial information at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud.

The likelihood of harm resulting from this incident is increased because the incident resulted from malicious action (deliberate attack) and the breach was not discovered for almost 4 months.

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 affected individuals were notified email on August 29, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner