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	Golf Avenue Inc. (Organization)
Decision number (file number)	P2021-ND-208 (File #019741)
Date notice received by OIPC	March 2, 2021
Date Organization last provided information	March 2, 2021
Date of decision	November 1, 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 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's head office is on Montreal Quebec. 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: • name, • address, • telephone number, • email address, • credit card and transaction information (date and time), and • account credentials. This information is about identifiable individuals 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.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On January 7, 2021, the Organization discovered a key logger on its e-commerce platform upon completing a routine vulnerability scan.

	• The Organization confirmed that, on December 27, 2020, an administrator account was used to upload a picture containing malicious PHP code to the Organization's catalog of website photos. • The malicious code acted as a key logger that captured the information entered by the Organization's customers upon checkout. • Customer personal information and payment details entered on the website between December 27, 2020 and January 7, 2021, may have been accessed without authorization.
Affected individuals	The incident affected 924 individuals, including 42 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Worked with independent cybersecurity experts to contain the incident. • Offered assistance to affected individuals, if required. • Implemented additional security measures for accounts, and implemented further segregation of the infrastructure. • Subscribed to additional cybersecurity services to enhance malware scanning capabilities and security patching procedures. • Enhanced payment process security.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on February 11, 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, *The possible consequences might include the loss of confidentiality of personal information, phishing or other social engineering attacks, or fraudulent transactions.* In my view, a reasonable person would consider that the contact and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. Further, credentials could be used to compromise other online accounts. These are all 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 reported, *While there is no indication that the personal information affected by the incident was or will be misused, there is a possibility that the harm described … could materialize, given the nature of the incident.* 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). The lack of reported incidents of identity theft or fraud to date is not a mitigating factor, as identity theft can happen months and even years after a data breach. Further, the information may have been exposed for approximately twelve (12) 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 individuals.

A reasonable person would consider that the contact and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. Further, credentials could be used to compromise other online accounts. These are all 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). The lack of reported incidents of identity theft or fraud to date is not a mitigating factor, as identity theft can happen months and even years after a data breach. Further, the information may have been exposed for approximately twelve (12) days.

I require the Organization to notify the affected individuals whose 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 email on February 11, 2021 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner