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	Char-Broil, LLC (Organization)
Decision number (file number)	P2017-ND-73 (File #005700)
Date notice received by OIPC	May 24, 2017
Date Organization last provided information	May 24, 2017
Date of decision	June 9, 2017
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 an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, • billing address, • telephone number, and • payment card number, expiry date, CVV2 code. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected from residents of Alberta via the Organization's e-commerce website.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• On April 21, 2017, the Organization discovered that an unauthorized third party uploaded malicious computer code to the system that hosts the Organization's website, Charbroil.com

	• The Organization believes the code was present when customers made purchases via the online store during approximately March 22, 2017 and April 21, 2017, and that the code may have been used to obtain customer payment card transaction information for a limited number of transactions during that time.
Affected individuals	The incident may have affected 24 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Took steps to remove the code, understand what occurred, how it may have impacted online customer purchases, and enhanced security measures. • Reported to law enforcement. • Working with payment card networks. • Strengthening security of ecommerce website. • Providing credit monitoring and identity theft protection to potentially affected customers. • Created a dedicated phone line for customers to ask questions.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on May 9, 2017.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to the 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 "Unauthorized use of payment card information can result in unauthorized charges on payment cards." I agree with the Organization. The financial information at issue could be used to cause the harms of identity theft, fraud and financial loss. 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 reported that it "is unable to definitively state whether any particular individual will suffer negative consequences from the incident. However, because information provided when making a purchase on Charbroil.com during the time period, including payment card information, may have been impacted, [the Organization] is notifying a broad group of individuals who may have been affected by the incident so that they may take proactive steps to ensure that their personal information remains secure." In my view, the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion and malware). The information was potentially exposed for one month before the incident was discovered.

DECISION UNDER SECTION 37.1(1) OF PIPA
Based on the information provided by the Organization and given the circumstances, I have decided that there is a real risk of significant harm to the affected individuals as a result of this incident. The financial information at issue could be used to cause the significant harms of identity theft, fraud and financial loss. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion and malware). The information was potentially exposed for one month before the incident was discovered. I require the Organization to notify affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation.* I understand the Organization notified affected individuals by letter on May 9, 2017. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner