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	HP Restaurant Group (Organization)
Decision number (file number)	P2019-ND-172 (File #013407)
Date notice received by OIPC	June 6, 2019
Date Organization last provided information	June 6, 2019
Date of decision	November 26, 2019
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 headquartered in Ohio, USA, and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	Information involved in the breach included: • name, • credit or debit card number, expiry date, and security code (or CVV), and • some customer user account names and passwords may also have been affected. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected via the Organization's ecommerce website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On or about April 5, 2019, the Organization was notified of suspicious activity regarding its online payment processing platform.

	• On or about April 29, 2019, an investigation determined it was possible that customer credit and debit card information for transactions that occurred on the Organization's ecommerce gift card website since 2011 may have been subject to unauthorized access and/or acquisition.
Affected individuals	The incident affected five (5) Alberta residents.
Steps taken to reduce risk of harm to individuals	• Immediately shut down the affected website and moved online gift card processing to a new environment. • Launched an investigation with the assistance of a third-party forensic firm. • Reported the incident to credit card companies and providing written notice to other state regulators and consumer reporting agencies, as required.
Steps taken to notify individuals of the incident	Affected individuals were provided with written notice beginning on May 24, 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 that it is "…is providing all impacted individuals with guidance on how to better protect against identity theft and fraud". In my view, a reasonable person would consider that the financial information at issue could be used to cause the harms of identity theft and fraud. Credentials could be used to compromise other online accounts. 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 did not specifically assess the likelihood of harm resulting from this incident. In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased as the breach appears to be the result of malicious intent (deliberate, unauthorized access/acquisition) and has been ongoing since 2011 (eight years).
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 financial information at issue could be used to cause the harms of identity theft and fraud. Credentials could be used to compromise other online accounts. These are significant harms.	

The likelihood of harm resulting from this incident is increased as the breach appears to be the result of malicious intent (deliberate, unauthorized access/acquisition) and has been ongoing since 2011 (eight years).

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 provided with written notice beginning on May 24, 2019. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner