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	Gentle Giant Studios, Inc. d/b/a Gentle Giant Ltd. (Organization)
Decision number (file number)	P2018-ND-062 (File #006708)
Date notice received by OIPC	October 20, 2017
Date Organization last provided information	October 20, 2017
Date of decision	June 18, 2018
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) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • address, • telephone number, • email address, • credit/debit cards, • expiration date, and • CVV numbers. 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 e-commerce website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• In August 2017, in response to customer reports of fraudulent activity on their credit/debit cards, the Organization conducted an investigation of its e-commerce website. • The investigation revealed that an unauthorized JavaScript link had been introduced to the "footer" of the website. The link was designed by an unauthorized third party to harvest data submitted via a web form and exfiltrate the data to the unauthorized third party. • The Organization determined that between April 24, 2017 and August 4, 2017, the unauthorized third party may have acquired information about Alberta residents who provided new or updated information. • There is no indication that there was exposure of any then-existing information that had been previously provided to the Organization.
Affected individuals	The incident affected 19 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Suspended acceptance of all payment via credit/debit cards through its e-commerce. • Notified credit card brands and credit/debit transaction processors. • Implemented increased security measures to protect the payment card data. • Provided notice to each of the affected customers.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter sent on October 3, 2017.
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 did not specifically identify any harm that might result from this incident, but its notification to affected individuals stated "Please carefully review all of your credit/debit card and other financial accounts. If you find suspicious activity, we encourage you to promptly call your credit card provider or financial institution and also report the suspicious activity to law enforcement." In my view, the financial information at issue (payment card numbers, security codes) could be used to cause the significant harms of fraud, identity theft and financial loss. The contact information at issue, as well as email address, could be used for unsolicited telephone calls, emails and phishing. I have previously found phishing to be a significant harm.

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 provide an assessment of the likelihood that significant harm would result from this incident. In my view, 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 unauthorized intrusion). Further, the information may have been exposed for approximately four 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.

The financial information at issue (payment card numbers, security codes) could be used to cause the significant harms of fraud, identity theft and financial loss. The contact information at issue, as well as email address, could be used for unsolicited telephone calls, emails and phishing. I have previously found phishing to be a significant harm. 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 unauthorized intrusion). Further, the information may have been exposed for approximately four months.

I require the Organization to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified affected individuals in letter dated October 3, 2017 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner