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	Conde Nast (Organization)
Decision number (file number)	P2019-ND-176 (File #013583)
Date notice received by OIPC	May 13, 2019
Date Organization last provided information	May 13, 2019
Date of decision	November 27, 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 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, • postal address, • email address, • payment card number, expiry date, and security code. 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 website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• Between April 14, 2019, and April 17, 2019, an unauthorized person(s) gained access to certain systems of the third-party vendor that maintains and operates certain subscription pages for the Organization and was able to modify certain subscription pages to acquire transaction information.

	• The Organization first learned of a potential incident on April 17, 2019, when a third-party provider of advertising services informed it that there was a policy violation/malvertising on a subscription page. • The vulnerabilities were removed on April 17, 2019. On April 24, 2019, the Organization was notified that there was a reasonable belief that the unauthorized code compromised transaction information.
Affected individuals	The incident affected approximately 1,161 individuals, including four (4) Alberta residents.
Steps taken to reduce risk of harm to individuals	• Reset all passwords used to access the systems impacted by the incident and implemented a stronger password policy. • Assessing additional steps to reduce the likelihood of a similar event happening again in the future. • Notified the payment card brands about the incident, and arranged for 1 year of dark web monitoring services for all affected Canadians at no cost.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on May 10, 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 individuals affected could be subject to fraudulent charges on their credit or debit cards during the time period before card companies issued new cards." In my view, a reasonable person would consider that the 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 "The risk is low because [the Organization] notified the payment card brands of the incident and suspects that the brands will reissue the cards." 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). Despite the fact the Organization "suspects that the [payment card brands] will reissue the cards", this does not mitigate the potential for identity theft, fraud and phishing which can occur months or even years after personal information is compromised.

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 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 as the breach appears to be the result of malicious intent (deliberate, unauthorized access). Despite the fact the Organization "suspects that the [payment card brands] will reissue the cards", this does not mitigate the potential for identity theft, fraud and phishing which can occur months or even years after personal information is compromised. 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 by email on May 10, 2019. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner