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	The Topps Company, Inc. (Organization)
Decision number (file number)	P2019-ND-122 (File #012110)
Date notice received by OIPC	February 21, 2019
Date Organization last provided information	February 21, 2019
Date of decision	August 1, 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"	The incident may have involved the following information: • name, • mailing address, • telephone number, • email address, and • payment card information (including credit/debit 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. To the extent this information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• On December 26, 2018, the Organization became aware of possible unauthorized access to the www.topps.com website.

	• On January 10, 2019, the Organization's investigation confirmed that an unauthorized third party placed malicious code at the website, which may have resulted in access to or acquisition of payment card and other information that customers provided when placing orders through the website between November 19, 2018 and January 9, 2019.
Affected individuals	The incident affected 5,700 individuals, including 5 whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Initiated an investigation and engaged a security firm to examine the network. Removed the malicious code and cut off all known means through which unauthorized parties could gain access to the website. • Worked with the security firm and its website development company to implement measures to strengthen the security of system and prevent a similar incident from happening again. • Upgraded the website platform.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on February 22, 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 "Potential harms to affected individuals include financial loss, fraud, and identity theft." Further, "Names, mailing addresses, and phone numbers are not, by themselves, highly sensitive information. Credit and debit card information is deemed more sensitive, and it is possible that an unauthorized third party accessed or acquired credit/debit card numbers, along with card expiration dates and security codes. E-mail addresses are also sensitive to the extent they could be used to conduct phishing attacks in an attempt to obtain more sensitive information from individuals." In my view, a reasonable person would consider that the contact and 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 fraud and identity theft.
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	The Organization reported that it… *…cannot confirm whether any personal information was accessed or acquired, but the investigation confirmed that this was possible during the relevant time period. The company has not identified the person(s) responsible or*

between the incident and the possible harm.	*recovered any customer information that was potentially acquired….Security measures, such as encryption, were in place, but the intruder installed malware that could enable information to be acquired as customers placed orders through the website.* *Based on the foregoing, it is difficult to assess with any degree of certainty the actual likelihood of harm. To be prudent, [the Organization] has taken the position that there is a reasonable chance that harm may result.* In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased as the breach appears to be the result of a deliberate, unauthorized intrusion and installation of malware. The information was exposed for over a month and a half.

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 significant harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to fraud and identity theft. The likelihood of harm resulting from this incident is increased as the breach appears to be the result of a deliberate, unauthorized intrusion and installation of malware. The information was exposed for over a month and a half.

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 that affected individuals were notified by letter on February 22, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner