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)	P2017-ND-33 (File #004701)
Date notice received by OIPC	January 6, 2017
Date Organization last provided information	January 6, 2017
Date of decision	February 21, 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"	Some or all of the following information was involved in this incident: • name, • address, • email address, • telephone number, • credit or debit card number, • expiry date, and • card verification number. 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 e-commerce website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• One or more intruders gained unauthorized access to the Organization's website (www.topps.com) and installed malware. • The intruder(s) may have accessed the information at issue for customers who placed orders through the website between approximately July 30, 2016 and October 12, 2016. • The Organization's website development company discovered the incident on October 12, 2016.
Affected individuals	The incident may have affected 41 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Immediately initiated an investigation. • Retained a security firm to examine the network. • Implemented measures to increase system security (including removing malware, updating security patches, installing additional monitoring processes, and performing more frequent security scans). • Provided CSID Protector services to affected individuals, including identity theft insurance and restoration coverage.
Steps taken to notify individuals of the incident	All potentially affected Canadians were notified by email sent January 6, 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 "Potential harms to affected individuals include financial loss, fraud and identity theft." Further "E-mail addresses are also sensitive to the extent they could be used by unauthorized persons to conduct phishing attacks in an attempt to obtain more sensitive information from individuals." I agree with the Organization's assessment. The financial information at issue could be used to cause the harms of identity theft, fraud or financial loss. In addition, email addresses could be used for phishing purposes. 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 "There is a reasonable likelihood of harm to individuals…" and noted "the intruders were able to unlawfully insert malware". Further, "The company has neither identified the person(s) responsible, nor recovered the customer information that was potentially accessed." I agree with the Organization's assessment. The likelihood of harm resulting from this incident is increased because there was malicious intent involved (deliberate intrusion and installation of malware) and the information may have been exposed for approximately 2.5 months. The responsible person(s) have not been identified and the customer information that was potentially accessed has not been recovered.

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 as a result of this incident. The financial information at issue could be used to cause the harms of identity theft, fraud or financial loss. In addition, email addresses could be used for phishing purposes. These are significant harms. The likelihood of harm resulting from this incident is increased because there was malicious intent involved (deliberate intrusion and installation of malware) and the information may have been exposed for approximately 2.5 months. The responsible person(s) have not been identified and the customer information that was potentially accessed has not been recovered. 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 that all potentially affected Canadians were notified by email sent January 6, 2017. The Organization is not required to notify affected individuals in Alberta again.

Jill Clayton
Information and Privacy Commissioner