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	RM Acquisition, LLC d/b/a Rand McNally (Organization)
Decision number (file number)	P2017-ND-69 (File #005578)
Date notice received by OIPC	May 10, 2017
Date Organization last provided information	May 10, 2017
Date of decision	May 31, 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"	The incident involved the following information: • first and last name, • address, • telephone number, and • credit or debit card information (card number, expiry, CVV). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected from residents of Alberta via the Organization's e-commerce website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On April 11, 2017, the Organization confirmed there was unauthorized remote access to its e-commerce store server www.RandMcNally.com. • The access began on April 12, 2016 and resulted in the installation of malware on the server.

	• The Organization determined that between April 12, 2016 and March 2, 2017, the malware collected or may have collected data relating to customers who made purchases through the e-commerce store using a credit card or debit card.
Affected individuals	The incident may have affected 110 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Retained third-party forensic investigation firm to assist with the investigation. • Removed malware. • Offering potentially affected individuals 1 year of free identity monitoring and identity restoration services. • Established a hotline for affected individuals with questions or concerns. • Notifying other state regulators and major consumer reporting agencies.
Steps taken to notify individuals of the incident	Affected individuals were notified by mailed written notice on May 5, 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 did not specifically identify any harm that might result from this incident but reported it was "providing potentially impacted individuals with helpful information on how to protect against identity theft and fraud…". In my view, the financial information at issue could be used to cause the harms of identity theft, fraud and financial loss. 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, the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion and malware). The information was potentially exposed for almost 11 months before the incident was discovered and has not been recovered.
DECISION UNDER SECTION 37.1(1) OF PIPA	
Based on the information provided by the Organization and given the circumstances, 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 significant harms of identity theft, fraud and financial loss. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion and malware). The information was potentially exposed for almost 11 months before the incident was discovered and has not been recovered.	

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

I understand the Organization notified affected individuals by mailed written notice on May 5, 2017. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner