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	MTG USA, Inc. (Organization)
Decision number (file number)	P2022-ND-077 (File #023185)
Date notice received by OIPC	September 21, 2021
Date Organization last provided information	September 21, 2021
Date of decision	January 10, 2023
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's head office is in Pasadena, California, USA. 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 some or all of the following information: • name, • address, and • credit card information. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information at issue was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization became aware of suspicious activity on its website and launched an investigation. • On September 9, 2021, its investigation confirmed that an attacker placed malicious code and JavaScript on its website, which was designed to capture payment card information.

	• The investigation concluded that the incident occurred between June 25, 2020, and June 15, 2021, potentially exposing certain transactions. • The specific cause has not been identified.
Affected individuals	The incident affected 4270 individuals including 11 individuals in Alberta.
Steps taken to reduce risk of harm to individuals	• Offered a complimentary two-year membership for identity theft protection. • Suspended credit card transactions from its e-commerce site. Shut down the site pending the forensic investigation and determination of the scope of the incident. • Selected a new payment gateway and elected security controls on the platform which exceed the minimum required settings. • Engaged a specialist on security issues. • Notified the FBI.
Steps taken to notify individuals of the incident	Affected individuals were notified by email and letter on July 7, 2021.
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, *While there is no evidence that any personal information was accessed, acquired or misused, unauthorized persons may have possibly obtained credit card information.* In my view, a reasonable person would consider that the contact and financial information at issue could be used to cause the harms of identity theft, fraud and financial loss. These are all 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 that the likelihood that the harm will result is, "*Unknown at this time*." In my view, a reasonable person would consider 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 intrusion). The lack of reported incidents of identity theft or fraud to date is not a mitigating factor in the likelihood of harm resulting from this incident. Identity theft can happen months and even years after a data breach. Further, the information may have been exposed for approximately one year.

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. Contact and financial information at issue could be used to cause the harms of identity theft, fraud and financial loss. These are all significant harms. 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 intrusion).The lack of reported incidents of identity theft or fraud to date is not a mitigating factor in the likelihood of harm resulting from this incident. Identity theft can happen months and even years after a data breach. Further, the information may have been exposed for approximately one year. I require the Organization to notify the affected individuals whose information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the Organization notified affected individuals by letter on September 21, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Information and Privacy Commissioner