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	CM Group Holdings, Inc. d/b/a Creative Memories (Organization)
Decision number (file number)	P2021-ND-105 (File #013053)
Date notice received by OIPC	April 11, 2019
Date Organization last provided information	April 11, 2019
Date of decision	March 31, 2021
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 operates is headquartered in Minnesota, USA, and 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, • credit or debit card number, expiry date, and security number or CVV. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• On or about February 19, 2019, the Organization identified suspicious activity regarding its online payment processing platform. • On or about March 4, 2019, the Organization's investigation determined that customer credit and debit card information for certain transactions that occurred on the ecommerce

	website between February 10, 2019 and February 14, 2019, and on February 19, 2019, may have been subject to unauthorized access and/or acquisition.
Affected individuals	The incident affected 19 individuals in Alberta.
Steps taken to reduce risk of harm to individuals	• Investigated with the assistance of a third-party forensic firm to determine the nature and scope of the breach. • Working to implement additional safeguards for the site. • Continuing to monitor the ecommerce environment to guard against suspicious activity. • Reported the incident to credit card companies.
Steps taken to notify individuals of the incident	Affected individuals were notified in writing on April 1, 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 that it was "...providing all impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank". In my view, a reasonable person would consider that the financial information at issue could be used to cause significant harms such as 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 did not specifically provide its assessment of the likelihood of harm resulting from this incident. In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because it appears to have resulted from malicious intent (deliberate unauthorized intrusion). The information was exposed for four days.
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 significant harms such as identity theft and fraud. The likelihood of harm resulting from this incident is increased because it appears to have resulted from malicious intent (deliberate unauthorized intrusion). The information was exposed for four days.	

The Organization is required 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 the affected individuals were notified in writing on April 1, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner