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	Master Paints Institute (MPI) Canada, Inc. (Organization)
Decision number (file number)	P2020-ND-038 (File #014105)
Date notice received by OIPC	December 6, 2019
Date Organization last provided information	December 6, 2019
Date of decision	April 1, 2020
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 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 involved all or some of the following information: • first and last name, • address, • city, • state / province, • zip code, • telephone number, • email address, • company, • date of birth, • credit or debit card type, number, expiry date, CVV, • name, address, postal code for credit / debit card holder. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The personal information was collected in Alberta via the Organization's website.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On November 14, 2019, the Organization discovered a vulnerability in the shopping cart function on its website that allowed an unauthorized user to record information in the shopping cart. The incident was discovered by a consumer using the site, who reported it to the Organization. • The Organization reported that an unauthorized individual or group extracted personal information by executing a vulnerability in the code of the third party used for the shopping cart function. • The investigation determined that the unauthorized person was able to obtain the personal information at issue during the period of March 1, 2019 through November 14, 2019. • The incident did not affect any other part of the site or other information maintained by the Organization.
Affected individuals	The incident affected 292 individuals of which 26 are residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Disabled the shopping cart function, preventing further access. • Contacting all affected individuals and provided with direct lines of communication to support resources. • Notifying credit card companies. • Implemented a new third party hosted shopping cart. • Performed penetration tests and vulnerability scans on all other web assets and remediated any vulnerabilities. • Developing a process to prioritize and remediate any vulnerabilities found in quarterly scans. • Offering credit monitoring services and complimentary dark web monitoring services to affected individuals, as well as additional information about identity theft, and credit alerts / freezes. • Implemented a remediation plan: - Suspended the current shopping cart. - Performed network and security scans across all webpages to detect vulnerabilities. - Changed computer, database and third party hosting credentials. - Added a web application firewall to store and domain webpages. - Added new secure hosted checkout pages to prevent future attacks.

Steps taken to notify individuals of the incident	Affected individuals were notified by email on December 6, 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 the possible harm that might result from this incident include "Hacker or hackers have access to personal and credit card info." In my view, a reasonable person would consider that the contact and financial information at issue (including payment card numbers, CVV codes and expiry dates) could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. 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 "Hacker or hackers have access to personal and credit card info and may potentially use it." In my view, 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). Further, the information may have been exposed for approximately seven months.
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 (including payment card numbers, CVV codes and expiry dates) could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. 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). Further, the information may have been exposed for approximately seven months. 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 the Organization notified affected individuals in an email on December 6, 2019 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner