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	Interstate Plastics, Inc. (Organization)
Decision number (file number)	P2018-ND-066 (File #007020)
Date notice received by OIPC	November 7, 2017
Date Organization last provided information	November 7, 2017
Date of decision	July 3, 2018
Summary of decision	There is a real risk of significant harm to the individual affected by this incident. The Organization is required to notify this individual 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: • name, • address, • payment card number, • expiration date, and • CVV number. This information is about identifiable individual and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta via the Organization's website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On or around July 24, 2017, the Organization identified suspicious code on its e-commerce website and determined it was a sophisticated cyber-attack.

	• The Organization removed the code and began investigating with the assistance of third-party forensic investigators. • Additional malicious code was identified on August 25, 2017. • The code was capable of collecting payment information entered into the website's customer check out page by customers. • The Organization determined that that this incident may impact payment cards used to make purchases on the e-commerce site between May 29, 2017 and August 25, 2017. • The incident did not impact customer information received by the Organization via telephone orders. • The Organization was unable to rule out that an unauthorized actor may have also accessed a database containing customer information for certain transactions earlier than July 24, 2017. The Organization will be providing notice to these customers as well.
Affected individuals	The incident affected 1 Alberta resident.
Steps taken to reduce risk of harm to individuals	• Engaged third-party forensic investigators. • Removed the malicious code. • Implemented additional procedures to further protect the security of customers debit and credit cards. • Notified state regulators and the major consumer reporting agencies. • Providing guidance to customers on how to better protect against identity theft and fraud, how to obtain a free credit check, and how to place a fraud alert and security freeze on one's credit file.
Steps taken to notify individuals of the incident	The affected individual in Alberta was notified by letter on October 27, 2017.
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 did not specifically identify any harm that might result from this incident, but its notification to affected individuals stated "Please review the enclosed *Steps You Can Take to Protect Against Identity Theft and Fraud* for additional information as to how to better protect against identity theft and fraud. We encourage you to remain vigilant against incidents of identity theft by reviewing your account statements regularly and monitoring your credit reports for suspicious activity." In my view, the financial information at issue (payment card numbers, security codes) could be used to cause the significant harms of fraud, identity theft and financial loss.

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 an assessment of the likelihood that significant harm would result from this incident 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 and installation of malware). Further, the information may have been exposed for approximately three 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 individual.

The financial information at issue (payment card numbers, security codes) could be used to cause the significant harms of fraud, identity theft and financial loss. 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 and installation of malware). Further, the information may have been exposed for approximately three months.

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

I understand the Organization notified the affected individual in a letter dated October 27, 2017, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner