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	Hyde's Distribution (Organization)
Decision number (file number)	P2020-ND-160 (File #015823)
Date notice received by OIPC	May 11, 2020
Date Organization last provided information	May 11, 2020
Date of decision	November 20, 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 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 is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, • address, • telephone number, • credit card account number, expiry date, and security code. 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 April 21, 2020, the Organization discovered that purchase orders made through the website www.zippo.ca using credit cards might have been at risk of compromise due to the actions of an unknown external third party.

	• The Organization was made aware that malware known as a web skimmer script was used on the website to steal personal and payment information. The unauthorized actor had access to the Organization's network between February 20, 2020 until April 23, 2020.
Affected individuals	The incident affected 1,131 individuals, including 124 in Alberta.
Steps taken to reduce risk of harm to individuals	• Took the website offline to prevent further unauthorized access. • Engaged a specialized forensic IT company to conduct investigation. • Notified the Organization's payment processor, which has taken the necessary measures to notify all credit card companies of the incident. • Conducting a review of security and cybersecurity measures. • Reviewing cybersecurity and privacy policies and procedures to ensure adequate data protection safeguards and security systems.
Steps taken to notify individuals of the incident	Affected individuals were notified in writing on May 11, 2020.
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, "since the information of the Customers involved in the Incident includes sensitive financial information, there is a risk fraud [sic] and financial loss". 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 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 it … *… is of the view that the likelihood that harm could result to the Customers is moderate. While [the Organization] has no evidence that the personal information at issue was removed from [the Organization's] systems, the personal information involved in the Incident is nonetheless sensitive and could be used for the purposes of fraud. The fact that the Incident was caused as a result of the actions of an unknown actor with malicious intent additionally increases the likelihood that harm could result to the affected individuals.*

	I agree with the Organization's assessment. 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). Further, the information was available to the unknown third party for approximately two 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 could be used to cause the harms of identity theft, fraud and financial loss. These are 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 was available to the unknown third party for approximately two months.

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 in writing on May 11, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner