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	Write-On Stationery Supplies Inc. (Organization)
Decision number (file number)	P2018-ND-085 (File #005634)
Date notice received by OIPC	May 18, 2017
Date Organization last provided information	May 18, 2017
Date of decision	July 18, 2018
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 pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization operates in Alberta and is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information. • name, • address, • contact information, • order details, • credit card information, and • other account information. This information is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization uses a third party service provider, Pixel Army, to host its ecommerce website www.write-on.ca, online payment processing and records for both online and offline customers.

	• On May 9, 2017, Pixel Army contacted the Organization to advise that there had been an intrusion. • On May 10, 2017, Pixel Army identified that there was evidence of credit card skimming on the website. • The Organization understands that Pixel Army became aware of the intrusion on May 5, 2017 and investigated with the assistance of a third party. The investigation determined an intruder had accessed the server and installed malicious software and server back doors. • The Organization understands that payments made by credit card between October 19, 2016 and May 10, 2017 may be at risk.
Affected individuals	The incident affected 2,197 individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Removed all malicious files and server 'back doors'. • Scanned all site files for malware and viruses. • Built a new server and migrated all site files and databases. • Restructured functions on the server so that different locations are used for content management system and main website files. • Added in additional firewall restrictions. • Installing more server structure changes and monitoring services. Considering a website code refresh.
Steps taken to notify individuals of the incident	Affected individuals were notified by email by May 23, 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 the type of harm that might result from this incident, but advised affected individuals to "… review and monitor your credit card statements" and to "Contact your local law enforcement if you detect any unauthorized activity or suspect you may be a victim of identity theft." In my view, the contact and financial information at issue could be used to cause the significant harms of identity theft, fraud 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 reported that "Given the financial information involved in the incident and the malicious nature of the intrusion, there would appear to be a real risk of significant harm for individuals making payments by credit card on and after October 19, 2016 until the Website was taken offline on May 10, 2017 and the issues remediated." 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 almost 7 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.

The contact and financial information at issue could be used to cause the significant harms of identity theft, fraud 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 almost 7 months.

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

I understand the Organization notified the affected individuals by email by May 23, 2017, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner