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	Plow and Hearth, LLC (Organization)
Decision number (file number)	P2018-ND-113 (File #006773)
Date notice received by OIPC	October 5, 2017
Date Organization last provided information	October 5, 2017
Date of decision	August 13 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 whose 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: • name, • address, • telephone number, and • payment card information (number, expiry date, and CVV verification code). This information is about identifiable individuals 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	• The Organization uses a third party service provider, Aptos, Inc., to provide a digital commerce platform that functions as the back-end for the Organization's online stores.

	• On August 24, 2017, Aptos notified the Organization that there had been a remote access intrusion that resulted in unauthorized access to online transaction data information provided by customers of the Organization. • The Organization reported that, according to Aptos' investigation, the intrusion began on approximately July 22, 2017 and ended on August 9, 2017. • Aptos discovered indications of the intrusion in August 2017.
Affected individuals	The incident affected approximately 8 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Engaged a leading cybersecurity firm. • Taken steps to secure systems. • Working with law enforcement in their investigation. • Provided free credit report annually from two national credit bureaus.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on October 2, 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 "We encourage you to remain vigilant by reviewing your account statements and monitoring your free credit reports." 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 unauthorized intrusion). Further, the information may have been exposed for approximately two weeks.
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 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 unauthorized intrusion). Further, the information may have been exposed for approximately two weeks.

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 a letter on October 2, 2017 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner