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	Dungarees LLC, a Missouri limited liability company ("Organization")
Decision number (file number)	P2017-ND-59 (File #001223)
Date notice received by OIPC	July 20, 2015
Date Organization last provided information	April 10, 2017
Date of decision	May 23, 2017
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 is incorporated in Missouri, USA. It 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, • billing information associated with debit or credit card, • mailing address, • email address, • debit card information, • credit card information (including security code and expiration date). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected from residents of Alberta via the Organization's website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On May 15, 2015, the Organization was notified by a customer about suspicious credit card activity. • The Organization investigated, and found that after a migration of the Organization's website from one server to another, the Organization was hacked by a foreign entity. A forensic investigation revealed that malware had been active between March 26, 2015 and June 5, 2015. • As a result, the Organization believes that its customers' personal information may have been accessed by an unauthorized third party during that time.
Affected individuals	There were a total of 11,564 affected individuals, including 48 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Immediately took action to secure website and initiated an investigation. • Notified all affected customers by email and provided a phone number to address customer questions. Customers were also invited to email the Organization. • Reported the incident to the United States Secret Service and the New Jersey State Police.
Steps taken to notify individuals of the incident	Affected individuals were notified by email sent on July 1, 2015.
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.	In its report of the incident, the Organization specified that customers may experience fraudulent charges on their debit card or credit card. In its notice to affected individuals, the Organization notes that "We recommend that you carefully review your account statements and monitor your credit reports." I agree with the Organization's assessment. The financial information at issue (including card security code and expiration date) could be used to cause the significant harms of identity theft and fraud. In addition, email addresses could be used to gain unauthorized access to other internet accounts and to cause the significant harm of phishing.

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 "It is possible that fraudulent charges could result. It is possible that the information may have been exposed for nine weeks. There was evidence of malicious code." 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 nine 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 (including card security code and expiration date) could be used to cause the significant harms of identity theft and fraud. In addition, email addresses could be used to gain unauthorized access to other internet accounts and to cause the significant harm of phishing. 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 nine weeks.

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 affected individuals in an email dated July 1, 2015, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner