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	B. Lane, Inc. d/b/a Fashion to Figure (Organization)
Decision number (file number)	P2017-ND-30 (File #001965)
Date notice received by OIPC	November 24, 2015
Date Organization last provided information	February 5, 2016
Date of decision	February 2, 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 a Delaware corporation and is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	Some or all of the following information was involved in this incident: • name, • customer ID, • address, • telephone number, • email address, and • credit card information. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected via the Organization's e-commerce website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On October 16, 2015, the Organization noticed that a page on its website, which was managed by a third party web hosting firm, was loading slowly. • An investigation was immediately conducted, which indicated that malware had been installed on the hosting firm's webserver on or around May 19, 2015. The information at issue was stored on the webserver. • The Organization reported that it "has not received any forensic evidence from its former third party web hosting firm establishing that such information was actually accessed without authorization", but also noted "it does not appear that the former third party web hosting firm conducted a forensic analysis in connection with this event."
Affected individuals	The incident potentially affected 15,111 individuals, including 3 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Took down the impacted website, and removed malware from the impacted webserver. • Completed an internal IT audit to identify and address any other vulnerabilities. • Retained a new web hosting firm. • Completed a number of additional security enhancements and provided employee training. • Provided identity protection services to affected individuals.
Steps taken to notify individuals of the incident	On November 13, 2015, the Organization mailed notification letters to all individuals who made online purchases between May 19, 2015 and October 16, 2015.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to the 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 "To the extent that unauthorized individuals successfully accessed [the Organization's] data, which has not been established, it is possible that impacted individuals could experience financial fraud." The Organization also noted "The risk of harm resulting from the potential exposure of names, Customer IDs, addresses, phone numbers, and e-mail addresses is low. There is no risk of damage, injury, or other detriment that could occur due to the disclosure of such information, particularly because most of these data elements are publicly available and cannot be used to commit identity theft or fraud. The risk of harm associated with an unauthorized access to names and credit card information, which has not been established, would be greater." In my view, the financial information at issue (credit card information), together with contact information, could be used to cause the harms of identity theft, fraud or financial loss. In addition, email addresses could be used for phishing purposes. 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 "the risk of fraud occurring is mitigated by the identity protection services provided by ID Experts at no cost to the impacted individuals." Further, the Organization said "If an individual has a confirmed instance of identity theft, ID Experts will assign the individual to their own personal Recovery Advocate, who will work with the individual throughout the resolution process." In my view, the likelihood of harm resulting from this incident is increased because there was malicious intent involved (deliberate intrusion and installation of malware) and the information was exposed for approximately 5 months. Although the Organization has committed to providing protection services and working with individuals who may experience identity theft, this will only apply where the Organization is made aware of such transactions. Further, this does not necessarily mitigate the potential harm that may result if information from the Organization's systems is used for identity theft or other forms of fraud, at other e-commerce sites, for example.

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 as a result of this incident.

The financial information at issue (credit card information), together with contact information, could be used to cause the harms of identity theft, fraud or financial loss. In addition, email addresses could be used for phishing purposes. These are significant harms. The likelihood of harm resulting from this incident is increased because there was malicious intent involved (deliberate intrusion and installation of malware) and the information was exposed for approximately 5 months. Although the Organization has committed to providing protection services and working with individuals who may experience identity theft, this will only apply where the Organization is aware of such transactions. Further, this does not necessarily mitigate the potential harm that may result if information from the Organization's systems is used for identity theft or other forms of fraud, at other e-commerce sites, for example).

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 that on November 13, 2015, the Organization mailed notification letters to all individuals who made online purchases between May 19, 2015 and October 16, 2015. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner