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	LA Fashion Enterprise Ltd. (Organization)
Decision number (file number)	P2018-ND-099 (File #009351)
Date notice received by OIPC	July 31, 2018
Date Organization last provided information	July 31, 2018
Date of decision	August 7, 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 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 headquartered in Manchester, UK 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, • email address, • home and/or delivery address, • telephone number, • where appropriate, company name and/or VAT ID, and • possibly credit or debit card details at the point of sale in the short period before the information is disposed of. 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, ww.lasula.co.uk. To the extent information was collected in Alberta, PIPA applies in this matter.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On June 4, 2018, the Organization was made aware that anomalous software had been installed on its server. • On June 28, 2018, the Organization's technical investigators confirmed the software had the capability to enable the intruder to gain access to customer databases containing personal information provided by customers when making online orders, and to intercept credit or debit card details at the point of sale. • The unauthorized access is believed to have taken place between December 7, 2017 and May 22, 2018. • The Organization is unable to definitively conclude whether personal data or debit/credit card details were in fact exfiltrated, but consider this to be likely as the attacker had the access and tools required.
Affected individuals	The credit card information of approximately 30,000 customers may have been compromised (including 84 individuals residing in Canada). The personal information (not credit card information) of approximately 240,000 customers may have been compromised (including approximately 535 individuals residing in Canada).
Steps taken to reduce risk of harm to individuals	• Removed the anomalous software. • Retained IT technical forensic providers to investigate. • Notified data protection authorities in the United Kingdom and Canada.
Steps taken to notify individuals of the incident	The Organization reported an email notification of the potential breach was sent to all customers whose personal information was stored in its database.
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 types of harm(s) that could result from this incident, but its notification to affected individuals said "You should check your credit and debit card statements over the past 9 months for any evidence of fraud. … You should consider cancelling any debit or credit cards used on www.Lasula.co.uk or www.Lasula.com accounts during the past 9 months." The Organization's notification to customers whose personal information was likely compromised (but not payment card information) advised as follows: "If you receive any communication that appears to be from [the Organization] which looks suspicious to you, please contact us."

	In my view, the financial information at issue (payment card information) could be used to cause the harms of identity theft and fraud. Contact information, and email address in particular, could be used for phishing purposes. These are all 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 attack to which [the Organization] has been subjected is likely to have been launched by criminals who specialise in exploiting weaknesses in proprietary extensions of Magenta software." Further, the Organization's third-party forensic investigators are unable "to definitively conclude whether personal data or debit/credit card details were in fact exfiltrated, but they consider this to be likely on the basis that the attacker had the access and tools required." 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). The information may have been exposed for over 5 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 financial information at issue (payment card information) could be used to cause the harms of identity theft and fraud. Contact information, and email address in particular, could be used for phishing purposes. These are all 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 and installation of malware). The information may have been exposed for over 5 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 an email notification of the potential breach was sent to all customers whose personal information was stored in the Organization's database. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner