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	Lulu's Fashion Lounge, Inc. (Organization)
Decision number (file number)	P2017-ND-58 File #003936)
Date notice received by OIPC	September 23, 2016
Date Organization last provided information	April 13, 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 the 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 the state of California 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, • billing address, • payment card number, • 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 customers making credit card transactions between August 11-16, 2016.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• One of the Organization's servers was compromised between August 11 and August 16, 2016, resulting in unauthorized access to personal information stored on it. • The Organization discovered the incident on August 23, 2016.
Affected individuals	52 individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Vulnerability on server patched and investigation launched. • Notified payment card issuing banks. • Set up a dedicated hotline for affected individuals to call to receive information. • Reported the incident to the Office of the Information and Privacy Commissioner of Alberta.
Steps taken to notify individuals of the incident	Notification sent by mail on September 23, 2016.
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.	In its report to the OIPC, the Organization indicated that this incident could "lead to unauthorized charges being made on potentially impacted customers' credit cards". In addition, the notification sent to the affected individual provided information for protecting oneself from identity theft, fraud and financial loss. In my view, the personal information involved could be used to cause the harms of identity theft, fraud and financial loss. 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 did not specifically assess the likelihood of harm resulting from this incident. It stated that "risk is mitigated by the brief time frame in which information was implicated (…) and the quick notification of the payment card network so that the credit card companies could monitor accounts for suspicious activity". In my view, the likelihood of harm resulting from this incident is increased because the incident resulted from malicious intent, and the information was exposed for 5 days and has not been recovered. Although the Organization notified the payment card network quickly, this does not necessarily mitigate the potential harm from identity theft or other forms of fraud.

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 individual. The personal information involved 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 incident resulted from malicious intent, and the information was exposed for 5 days and has not been recovered. Although the Organization notified the payment card network quickly, this does not necessarily mitigate the potential harm from identity theft or other forms of fraud. 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 in a letter dated September 23, 2016, in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner