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	LaCie USA (Organization)
Decision number (file number)	P2015-ND-07 (File #P2665)
Date notice received by OIPC	April 16, 2014
Date Organization last provided information	October 29, 2014
Date of decision	February 24, 2015
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 Oregon, USA. I have jurisdiction because the Organization is an "organization" as defined in section 1(1)(i)(i) of PIPA and the personal information was collected in Alberta.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, • mailing address, • email address, • credit card number and expiration date. This information is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On March 19, 2014, the Federal Bureau of Investigation (FBI) informed the Organization that sometime between March 27, 2013 and March 10, 2014, an unauthorized individual or group used malware to gain access to information from customer transacations made through the Organization's website. • The customer information was stored in a database and included: name, mailing address, email address, credit card number and expiry date. As well customers' website user names and passwords could have been accessed. • The information was not password protected, nor encrypted.
Affected individuals	In total, 160 individuals in Alberta were affected.
Steps taken to reduce risk of harm to individuals	• Customer passwords were all reset and a forensic firm retained to implement additional security measures. • A dedicated call centre was set up for concerned individuals to call with questions regarding the incident.
Steps taken to notify individuals of the incident	The Organization notified all affected individuals on April 14, 2014 by letter.
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 submitted there was a low level of harm to individual as a result of this incident. In my view, the personal information involved is of high sensitivity. It includes credit card numbers and expiry dates. This information could be used to cause harm in the form of identity theft and/or financial fraud. 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 there is a low likelihood that harm could result from this incident given the data involved. In my view, the likelihood of harm resulting from this incident is increased because the information was not encrypted nor password protected, and the incident resulted from malicious intent (installation of malware). In addition, the Organization was not aware of the breach until advised by law enforcement.

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. In coming to this decision, I considered the following factors: the personal information at issue could be used to cause identity theft and/or financial fraud and was not encrypted nor password protected. The incident was the result of malicious intent (installation of malware). The Organization was not aware of the breach until advised by law enforcement. The Organization notified the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation) on April 14, 2014. The Organization is, therefore not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner