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	prAna (Organization)
Decision number (file number)	P2017-ND-48 (File #005146)
Date notice received by OIPC	March 9, 2017
Date Organization last provided information	March 9, 2017
Date of decision	April 10, 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 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, • address, • telephone number, • email address, • username and account password for the website, and • payment card number, expiration date and security code (CVV). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta via the Organization's e-commerce website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On February 6, 2017, the Organization detected that an unauthorized third party may have obtained access to the servers that operate its e-commerce website, www.prana.com.

	• The Organization investigated and found that an unauthorized third party installed code that was designed to capture information as it was being entered on the site during the checkout process for orders placed from December 14, 2016 to February 6, 2017. • The Organization believes the unauthorized third party may have also decrypted an internal database containing information from orders completed prior to February 6, 2017.
Affected individuals	There are 1,669 affected individuals in Alberta.
Steps taken to reduce risk of harm to individuals	• Investigated and retained a cybersecurity firm to assist in the investigation and remediate the website. • Enhanced website security. • Notified the FBI. • Requiring users to change their passwords for the Organization's website, and recommending they do so across other accounts. • Provided a toll-free number that potentially affected customers can call with questions regarding the incident.
Steps taken to notify individuals of the incident	The Organization reported that it "is mailing a letter to all affected individuals in Alberta" and provided a draft of the notification letter.
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 that "The order information affected here includes payment card information which is generally used to make fraudulent purchases elsewhere on line." The Organization also reported "There may be some inconvenience associated with a replacement card, but that is not significant harm." In my view, the financial information at issue could be used to cause the harms of identity theft, fraud and financial loss. In addition, email addresses could be used for phishing purposes. Credentials (usernames and passwords) could be used to compromise other online accounts. 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 "Given that in Canada there is zero liablity [sic] for fraudulent credit card purchases made on an individual's credit card, there is no risk of significant harm to the affected individual [sic] in Alberta arising from this incident. The affected individual [sic] will be made whole by their credit card issuer." In my view, the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion and malware) and the information was potentially exposed for almost 2 months before the incident was discovered.

	The Organization can only speculate that affected individuals will not be held responsible for fraudulent credit card purchases, if such transactions are detected. Even if this were the case, it 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, 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 could be used to cause the harms of identity theft, fraud and financial loss. In addition, email addresses could be used for phishing purposes. Credentials (usernames and passwords) could be used to compromise other online accounts. These are significant harms. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion and malware) and the information was potentially exposed for almost 2 months before the incident was discovered. The Organization can only speculate that affected individuals will not be held responsible for fraudulent credit card purchases, if such transactions are detected. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud.

I require the Organization to notify affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* and provide me with written confirmation that it has done so on or before April 28, 2017.

Jill Clayton
Information and Privacy Commissioner