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	Spiraledge, Inc. (Organization)
Decision number (file number)	P2017-ND-125 (File #004847)
Date notice received by OIPC	January 27, 2017
Date Organization last provided information	August 10, 2017
Date of decision	August 28, 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"	Organization is incorporated and operating out of Campbell, CA, 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 the following information: • name, • address, • telephone number, • email address, 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 October 31, 2016, the Organization began investigating unusual activity reported by its credit card processor.

	• On November 28, 2016, the Organization confirmed that malware may have stolen credit or debit card data from some credit and debit cards used at the Organization's websites, www.swimoutlet.com and www.yogaoutlet.com, between May 2, 2016 and November 22, 2016.
Affected individuals	The incident affected 523 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Engaged third party forensic investigators. • Removed the malware to prevent further unauthorized access. • Worked with law enforcement to investigate the incident. • Established a hotline for customers with questions or concerns regarding the incident. • Notified other state regulators and the national consumer reporting agencies as necessary.
Steps taken to notify individuals of the incident	Notification was sent to affected customers by mail on January 12, 2017.
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 assess the harm that might result from this incident, but reported that it was "providing potentially impacted individuals with helpful information on how to protect against identity theft and fraud, including how to place a fraud alert and security freeze on one's credit file…". In my view, the contact and identity information at issue could be used to cause the harms of identity theft and fraud. 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 did not specifically assess the likelihood of harm resulting from this incident. 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 exposed for approximately 6 months. The Organization received reports of unusual activity that led to an investigation and discovery of the incident.
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 contact and identity information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes. 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 exposed for approximately 6 months. The Organization received reports of unusual activity that led to an investigation and discovery of the incident.

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 affected individuals were notified by mail on January 12, 2017. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner