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	MicroDAQ.com Ltd. (Organization)
Decision number (file number)	P2017-ND-41 (File #004220)
Date notice received by OIPC	November 2, 2016
Date Organization last provided information	November 2, 2016
Date of decision	March 6, 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"	The following information was involved in this incident: • name, • address, • credit card number, • security code (CVV), • expiry date, and • email address. 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 ecommerce website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On September 22, 2016 customers of the Organization reported credit cards being used in a fraudulent way. • The Organization learned that a third party embedded malware onto its ecommerce website that apparently caused some customers' financial information to be covertly sent to an unassociated email address. • Customers who purchased products from the Organization's website, www.MicroDAQ.com, between September 4 and September 22, 2016 may have been affected.
Affected individuals	A total of 13 Canadians were affected, including 2 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Conducted an investigation. • Reported incident to law enforcement. • Removed the malicious code that caused the breach. • Monitoring website and systems for evidence of any further breaches or exfiltration of data.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on or around November 1, 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.	The Organization reported "the possible harms would be limited to unauthorized use of those credit cards accounts. The contact information may be used to contact the individuals, exposing them to possible increased risk of phishing." I agree with the Organization's assessment. Financial information (credit card information) could be used to cause fraud and financial loss, as well as identity theft. 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 reported "That the information was compromised in connection with a malware installation that presumably took place for unlawful purposes, the likelihood that the information may be used for such criminal purposes may be presumed." The Organization also reported that it discovered the incident when "A couple of customers notified us regarding their credit card being used in a fraudlent [sic] way." I agree with the Organization. The likelihood of harm is increased because the incident resulted from malicious intent (deliberate intrusion and installation of malware). The information was exposed for over 2 weeks. The information was sent outside the Organization and has not been recovered, and it appears it was used for fraudulent purposes.

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. Financial information (credit card information) could be used to cause fraud and financial loss, as well as identity theft. Email addresses could be used for phishing purposes. These are significant harms. The likelihood of harm is increased because the incident resulted from malicious intent (deliberate intrusion and installation of malware). The information was exposed for over 2 weeks. The information was sent outside the Organization and has not been recovered, and it appears it was used for fraudulent purposes. 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 affected individuals by letter on or around November 1, 2016. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner