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	Mohu, an unincorporated division of Greenwave Scientific, Inc. (the Organization)
Decision number (file number)	P2016-ND-55 (File #001631)
Date notice received by OIPC	August 25, 2015
Date Organization last provided information	August 25, 2015
Date of decision	August 29, 2016
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 incident involved the following information: • name, • address, • email address, • telephone number, • credit card information, including card number, expiry date and CVV code. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA, collected from customers who purchased products from the Organization's website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• Between June 3, 2015 and July 28, 2015, the Organization's computer systems were compromised by a hacker who inserted malicious code and removed data. • The Organization's IT personnel discovered the data breach on July 28, 2015, during a review of the website's performance.
Affected individuals	A total of 2,500 individuals in North America were affected, including 3 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• The malicious code was removed from the system. • Additional security measures were added to the electronic systems. • The incident was reported to the Federal Bureau of Investigation, the United States Secret Service and state law enforcement agencies. • Credit reporting agencies were notified. • Affected individuals were offered a one year membership with a credit monitoring service.
Steps taken to notify individuals of the incident	Affected individuals were notified by mail sent August 10, 2015.
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 reported that "Impacted individuals may suffer identity theft, fraud, financial loss and/or negative effects on a credit record." I agree with the Organization's assessment. The incident involves financial information that could be used to cause the harms of identity theft, fraud, and financial loss. In addition, email addresses could be used to cause the harm of phishing. These are all 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 it believes "that the harm is not likely to be significant because (i) bank and credit card policies limit the financial losses that an individual may suffer from credit card fraud and misuse, (ii) the ability of the impacted individuals to cancel the effected credit cards, (iii) the ability of the impacted individuals to initiate a credit freeze, and (iv) [the Organization] has arranged for 12 months of free credit monitoring for each impacted individual."

	In my view, the likelihood of harm resulting from this incident is increased because the personal information was accessed in an unauthorized manner with malicious intent, and was exposed for almost two months before the Organization became aware of the breach. The Organization can only speculate that affected individuals will not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud, or use of the information for phishing 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.

The incident involves financial information that could be used to cause the harms of identity theft, fraud, and financial loss. In addition, email addresses could be used to cause the harm of phishing. These are all significant harms. The likelihood of harm resulting from this incident is increased because the personal information was accessed in an unauthorized manner with malicious intent, and was exposed for almost two months before the Organization became aware of the breach. The Organization can only speculate that affected individuals will not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud, or use of the information for phishing purposes.

I require the Organization to notify the affected individuals 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 August 10, 2015. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner