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	Web.com Group, Inc. (Organization)
Decision number (file number)	P2016-ND-65 (File #001364)
Date notice received by OIPC	August 18, 2015
Date Organization last provided information	July 28, 2016
Date of decision	December 20, 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 incorporated in Delaware and operates in Alberta. It is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • address, and • credit card information. 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.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On August 13, 2015, through ongoing security monitoring of its network, the Organization discovered unusual traffic to sensitive computer systems. • The Organization determined that a successful attack against its networks may have resulted in unauthorized access to some of its customers' personal information.

	• Upon discovery, the Organization immediately suspended the compromised computer systems, and started working with a forensic IT specialist to remediate the issue.
Affected individuals	The incident affected 696 individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Provided individuals with one year of free credit monitoring services. • Reported the incident to the Office of the Information and Privacy Commissioner of Alberta, as well as federal and local authorities in the USA.
Steps taken to notify individuals of the incident	Affected individuals were notified by email and mail on August 18, 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.	In assessing the type of harm that might result from the breach, the Organization reported the "level of sensitivity could be financial loss, fraud, identity theft, and negative effects on a credit report" and also "we believe the harm is not significant due to its early discovery and the immediate reporting to the credit card companies and credit bureaus." I agree with the Organization that the personal information involved could be used to cause the harms of identity theft, fraud, financial loss and negative effects on a credit report. 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.	As noted, the Organization reported "we believe that the harm, if any, would not be significant due to the early detection of the breach, and the immediate notification to the credit card companies and credit bureaus." In my view, the risk of harm resulting from this breach is increased given the incident resulted from the malicious action of an unknown third party and the personal information has not been recovered. While it may be that the swift discovery of the incident and reporting to credit card companies and credit bureaus reduces the likelihood of harm somewhat, it does not necessarily mitigate the risk that significant harm will result from this incident, which can happen months and even years after a data breach. To this end, the Organization advised affected individuals to remain vigilant for signs of fraudulent activity associated with their credit card information.

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 personal information involved could be used to cause the significant harms of identity theft, fraud, financial loss and negative effects on a credit report. The risk of harm resulting from this breach is increased given the incident resulted from the malicious action of an unknown third party and the personal information has not been recovered. While it may be that the swift discovery of the incident and reporting to credit card companies and credit bureaus reduces the likelihood of harm somewhat, it does not necessarily mitigate the risk that significant harm will result from this incident, which can happen months and even years after a data breach. To this end, the Organization advised affected individuals to remain vigilant for signs of fraudulent activity associated with their credit card information. 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 and email dated August 18, 2015, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner