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)	P2020-ND-039 (File #014092)
Date notice received by OIPC	December 4, 2019
Date Organization last provided information	December 4, 2019
Date of decision	April 1, 2020
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 whose personal information was collected in Alberta, 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) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • address, • telephone number, • email address, and • services offered to the account holder. The Organization reported that passwords and credit card information were encrypted, and not compromised as a result of the incident. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On October 16, 2019, the Organization became aware that a third-party might have gained unauthorized access to a limited number of its computer systems in late August 2019, and, as a result, account information may have been compromised. • The Organization reported that access was facilitated via two externally facing servers that were compromised through a web-enabled application vulnerability and a deprecated user credential. • The accessed computer systems also included Web.com's retail domain registrars, Network Solutions, Register.com, and NameSecure.
Affected individuals	The incident affected 39,527,385 individuals, of which 108,107 reside in Alberta
Steps taken to reduce risk of harm to individuals	Among other things, the Organization reported that it: • Took immediate steps to stop the intrusion and engaged a cybersecurity firm to investigate and determine the scope of the incident. • Worked with US federal law enforcement. • Notified merchant processor and relevant consumer credit agencies. • Required all users to reset password accounts and changed various passwords. • Updated formal information security plan. • Revised policies and procedures. • Implemented periodic technical and nontechnical evaluations/risk analyses/penetration tests. • Created and executed containment plans. • Implemented new technical safeguards. • Created clones of all affected systems for further forensic investigation.
Steps taken to notify individuals of the incident	Affected individuals were notified by email, online account manager, and through several company websites between October 29, 2019 and November 5, 2019.

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 "Possible harms may include phishing or similar attempts using contact information." I agree with the Organization's assessment. A reasonable person would consider the contact and profile information at issue, particularly in conjunction with email addresses, could be used for phishing purposes, increasing vulnerability to identity theft and fraud. 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 "Due to the access being limited to basic contact information and services descriptions, the encryption of credit card numbers and passwords, and the mitigation efforts undertaken following discovery, including but not limited to the mandatory password reset for each account, the company does not consider there to be any real risk of significant harm to affected individuals". In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). Further, the information may have been exposed for approximately two months.

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.

A reasonable person would consider the contact and profile information at issue, particularly in conjunction with email addresses, could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). Further, the information may have been exposed for approximately two months.

I require the Organization to notify the affected individuals whose personal information was collected in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified affected individuals by email, online account manager, and through several company websites between October 29, 2019 and November 5, 2019, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner