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	Weebly, Inc. (Organization)
Decision number (file number)	P2017-ND-16 (File #004647)
Date notice received by OIPC	December 23, 2016
Date Organization last provided information	December 23, 2016
Date of decision	January 11, 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 a U.S. company based in San Francisco and is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	Some or all of the following information was involved in this incident: • email addresses and/or usernames, • last login IP addresses, and • passwords that were either hashed or hashed and salted. 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 online website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization provides an on-line platform, Weebly.com, that enables individual and business users to create their own websites. • On October 8, 2016, the Organization was informed by LeakedSource.com that a file containing the information at issue from the Organization's database was copied by an unauthorized party and made available on the dark web.

	• The unauthorized access to the information at issue is believed to have occurred between October 2015 and February 2016. • No payment card data or data about end-users (eCommerce customers) was involved.
Affected individuals	The Organization reported it has approximately 99,000 users in Alberta.
Steps taken to reduce risk of harm to individuals	• Engaged a third party forensics firm to investigate. • Notified affected individuals. • Posted a security update banner online, as well as FAQs about the incident. • Enforced stronger user password requirements, and reminded users of the risks of using the same password across multiple sites (encouraged users to use unique passwords).
Steps taken to notify individuals of the incident	All potentially affected individuals were notified of the incident by email sent October 20, 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 that it "does not believe that the Incident poses a real risk of significant harm to Users in Alberta given the non-sensitive nature of the Data." The Organization "became aware of a phishing email that was sent to some of its Users on or around October 20, 2016. However, [the Organization] has no evidence to link the phishing email to the Incident (although it's possible the emails were sent because the phisher knew that [the Organization] had just publicly announced the Incident). [The Organization] has not received any indication that any User in Alberta received a phishing email." In my view, the email addresses at issue in this incident could be used to cause significant harm through phishing.
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 company has not received any User complaints from Alberta residents, and there has been no evidence of misuse of the personal information in question." 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 public posting of the information on the dark web), the number of potentially affected individuals, and the information may have been exposed for almost 1 year. Although the Organization is not aware of any Alberta users experiencing phishing attempts, this does not mean this has not or will not occur.

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 as a result of this incident. The email addresses at issue in this incident could be used to cause significant harm through phishing. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion and public posting of the information on the dark web), the number of potentially affected individuals, and the information may have been exposed for almost 1 year. Although the Organization is not aware of any Alberta users experiencing phishing attempts, this does not mean this has not or will not occur. 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 all potentially affected individuals of the incident by email sent October 20, 2016. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner