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	Houzz Inc. (Organization)
Decision number (file number)	P2021-ND-086 (File #011930)
Date notice received by OIPC	February 1, 2019
Date Organization last provided information	February 1, 2019
Date of decision	March 16, 2021
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 a U.S. corporation headquartered in Palo Alto, California and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • first name, last name, city, province/territory, country, "About Me" profile description (if provided by the user); • internal identifiers and fields (e.g., country of site used, whether a user has a profile image), • account information (i.e. email address, user ID, prior usernames, one-way hashed passwords and unique per user salt, last known IP address, general location information inferred from a user's IP address (i.e. city and approximate postal area), date and time that account was last updated, date and time account was created, current account status (i.e. active/inactive) and certain account information available to the public (i.e., current username and, if a user logs in through Facebook Login, the user's publicly available Facebook ID). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.

	The Organization maintains that "it is not subject to the jurisdiction of the Office of the Privacy Commissioner of Alberta in relation to this incident", but did not explain why it believes this to be the case. In my view, the Organization is an "organization" as defined in PIPA, and the information at issue is "personal information" as defined in PIPA. To the extent the personal information was collected in Alberta by the Organization, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• The Organization was contacted by a security researcher from a reputable security research firm under "responsible security disclosure" principles about a data file the researcher had obtained. • The file was provided to the Organization on December 18, 2018 in a password-protected form and appeared to contain an Organization user table. The Organization was able to confirm its authenticity on December 19, 2018. • The Organization reported its investigation is ongoing.
Affected individuals	The Organization reported it "…believes that, at most, 2.8 million Canadian residents have been affected by the incident, including Alberta residents". The Organization also said it "… does not have an estimate of the number of Alberta residents that may have been affected, though it is working to prepare such an estimate and will provide an update once available."
Steps taken to reduce risk of harm to individuals	• Initiated an investigation with the assistance of outside counsel and forensic investigators. • Required some users to reset their passwords and strengthened new password requirements. • Reported the incident to law enforcement and co-operating with authorities. • Committed to further enhancing safeguards.
Steps taken to notify individuals of the incident	The Organization reported that it is "(a) in the process of notifying all affected users, and (b) recommending that users reset their passwords." The Organization provided the text of its notification to affected individuals.

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 the personal information at issue "is non-sensitive in nature". The Organization also said "In addition, because [the Organization] stores hashes of user passwords with unique salts per user, it would be both computationally infeasible to reverse engineer the hashed values and extremely difficult to use pre-computed password databases or rainbow tables to use reverse lookup techniques to determine the original passwords." Further, "With respect to the email addresses involved in this incident, there remains a minimal risk that users could be targeted with a phishing attack." In my view, a reasonable person would consider the contact and account information at issue, and particularly email addresses and partial credentials (usernames), could be used for phishing purposes, increasing vulnerability to identity theft and fraud, and to compromise other online accounts. These are significant harms. I accept that it is unlikely hashed and salted passwords could be reverse engineered and used to cause significant harm.
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 "With respect to the email addresses involved in this incident, there remains a minimal risk that users could be targeted with a phishing attack. This risk is mitigated in part through the notice sent to affected individuals, and the absence of any malicious intent by the reputable security research firm that contacted us under the "responsible security disclosure" principles. In addition, even in a phishing context, [the Organization] is not generally a platform where users share sensitive personal information. In this context, the residual risk of harm to individuals as a result of the incident is low." In my view, a reasonable person would consider the risk of harm is increased as there has been unauthorized access to the personal information at issue and it appears the Organization does not know how this occurred. The Organization did not report how long the information was exposed before the breach was reported to it by a third party. I agree with the Organization that notifying affected individuals will help to mitigate the likelihood of significant harm resulting from this breach.
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 breach. A reasonable person would consider the contact and account information at issue, and particularly email addresses and partial credentials (usernames), could be used for phishing purposes, increasing vulnerability to identity theft and fraud, and to compromise other online accounts. These are	

significant harms. I accept that it is unlikely hashed and salted passwords could be reverse engineered and used to cause significant harm.

The risk of harm is increased as there has been unauthorized access to the personal information at issue and it appears the Organization does not know how this occurred. The Organization did not report how long the information was exposed before the breach was reported to it by a third party. I agree with the Organization that notifying affected individuals will help to mitigate the likelihood of significant harm resulting from this breach.

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 affected individuals were notified by email on February 28, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner