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	HomeStars, Inc. (Organization)
Decision number (file number)	P2019-ND-205 (File #013507)
Date notice received by OIPC	October 16, 2019
Date Organization last provided information	October 31, 2019
Date of decision	December 18, 2019
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 operates HomeStars.com, a free service to help homeowners find reputable renovators, repairmen and retailers, and 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: Users: • name, • address, • email address, • telephone number, • user ID, and • IP address. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. Service Professionals: Company information (including name, postal code, telephone number, country address, province, city, service area, owner name, telephone number, email address, ID, contact cell number, fax number, year established, number of employees, salesforce ID, Zuora ID, credit card first six digits, credit card last four digits, GST/HST, URL, user ID).

	Some of this information appears to qualify as "business contact information" which is defined in section 1(1)(a) of PIPA to mean "an individual's name, position name or title, business telephone number, business address, business email address, business fax number and other similar business information." Section 4(1)(d) of PIPA says that the Act does not apply to the collection, use and disclosure of business contact information "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." In this case, I considered that the possible unauthorized access to the information was not a collection, use or disclosure "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." Therefore, I find that PIPA applies to the personal information of service professionals in this instance, to the extent the personal information was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On September 30, 2019, the Organization discovered unauthorized activity that may have resulted in unauthorized access to one of the Organization's servers. • The Organization's investigation determined that the unauthorized activity began on September 28, 2019 and continued at least until October 2, 2019. • The incident occurred as a result of the unauthorized user exploiting a vulnerability in an open source data structure store, which was then used to access the affected underlying staging server by compromising authentication controls. The unauthorized access appears to allow equivalent access to the server as authorized users. • This unauthorized activity was discovered by the Organization's engineers who were unable to log into the server. Upon review, it was determined that the authentication file containing permissions for the approved users had been replaced.
Affected individuals	The incident affected 47,954 users, including 3514 users residing in Alberta.

Steps taken to reduce risk of harm to individuals	• Reset passwords. • Monitoring the "Dark Web" for evidence that information collected from the unauthorized activity is available or has otherwise been compromised. • Review of security systems and ongoing evaluation of enhancements and recommendations. • Notified the Office of the Privacy Commissioner of Canada.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on October 30, 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 "Any possible resulting harm from the unauthorized activity appears to be limited at the moment. Early analysis has produced no evidence of unauthorized access to or disclosure of personal information or that any information other than common, publicly available information was available on the database, beyond certain truncated credit card information that would not allow unauthorized financial activity." The Organization's notice to affected individuals, however, recommended they "Report any suspicious transactions or activities on your accounts to the appropriate companies and authorities", "Don't click on links or open attachments in unsolicited emails and text messages" and "Only use secure WiFi connections when making online purchases or checking bank accounts." In my view, a reasonable person would consider that the contact information at issue, including email address, could be used for the purposes of phishing, increasing the affected individuals' 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 did not specifically provide an assessment of the likelihood that significant harm would result from this incident. 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). The information may have been exposed for at least five days. Although the Organization reported there is "no evidence of unauthorized access to or disclosure of personal information", the Organization did not report on any technical controls (such as audit logs) that could evidence that the information was not accessed.

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 that the contact information at issue, including email address, could be used for the purposes of phishing, increasing the affected individuals' 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). The information may have been exposed for at least five days. Although the Organization reported there is "no evidence of unauthorized access to or disclosure of personal information", the Organization did not report on any technical controls (such as audit logs) that could evidence that the information was not accessed or exfiltrated. 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 were notified by email on October 30, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner