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	TaskRabbit, Inc. (Organization)
Decision number (file number)	P2021-ND-303 (File #019445)
Date notice received by OIPC	February 11, 2021
Date Organization last provided information	February 11, 2021
Date of decision	March 3, 2022
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 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: <u>Independent Contractors and Clients</u> • full name, • postal code, • telephone number, • email address, and. • identification number. <u>Taskers only</u>: • date of birth, and • bank account routing number. <u>Clients only:</u> • the last four digits of credit card number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies. Some of the information may 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 e mail 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 "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." As a result, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On December 7, 2020, the Organization experienced a spike in unusual traffic in the login endpoints for the Organization's client and tasker mobile applications. • The Organization determined that its website and mobile application had been subject to a credential stuffing attack on certain user accounts between December 7 - 14, 2020. • The Organization reported it believes the credentials were obtained from a third-party site or app where users used the same password.
Affected individuals	The incident affected 15 individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Reset user passwords and invalidated the sessions of any user account that was accessed (whether legitimate or otherwise) during the attack period. • Restricted the number of failed login attempts, reducing the nature and amount of data accessible at the login endpoints. • Updated the mobile application with additional security features. • Monitoring accounts for suspicious activity. • Implementing an invisible RECAPTCHA on all web login endpoints. • Reducing the nature and amount of data accessible at login endpoints. • Advised users to take extra security steps (e.g. complex passwords, never reuse passwords across different websites or applications.)

	• Encouraged users to enable two-factor authentication for their account (and any other service that offers it).
Steps taken to notify individuals of the incident	Affected individuals were notified by email on February 10, 2021.
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 did not specifically identify any harms that might result from this incident, but its notification to affected individuals said: *…we encourage you to be careful about any emails or calls you receive asking for personal information. Always verify the identity of the requester, and keep in mind that most legitimate businesses will not require you to provide personal information (including usernames/passwords) via email.* The Organization also reported that its notice to affected individuals "… reminds users not to re-use passwords across different websites or apps to better protect their accounts." In my view, a reasonable person would consider that the contact, identity and financial information at issue, particularly in conjunction with email address, could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. Confirmed valid credentials could be used to compromise other online accounts. 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 assess the likelihood that significant harm would result from this incident, but its notice to affected individuals said: *While we do not have any evidence or reason to believe that your personal information has been or will be misused, we suggest that you take extra security steps…* In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (brute force attack, credential stuffing) by an unknown third party who had already stolen individuals' credentials to be used for fraudulent purposes. The information may have been exposed for approximately one (1) week.

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, identity and financial information at issue, particularly in conjunction with email address, could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. Confirmed valid credentials could be used to compromise other online accounts. These are significant harms. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (brute force attack, credential stuffing) by an unknown third party who had already stolen individuals' credentials to be used for fraudulent purposes. The information may have been exposed for approximately one (1) week. 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 on February 10, 2021, in accordance with the Regulation. The Organization is not required to notify these affected individuals again.

Jill Clayton
Information and Privacy Commissioner