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	Airbnb Ireland UC ("Organization" or "Airbnb")
Decision number (file number)	P2021-ND-250 (File #020684)
Date notice received by OIPC	April 13, 2021
Date Organization last provided information	October 14, 2021
Date of decision	January 31, 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 the 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 reported that it "is an online vacation and rental marketplace. It hosts personal profiles and listings, maintains a smart messaging system so hosts and guests can communicate, and manages a trusted platform to collect and transfer payments." The Organization also said… *…it is the Company's respectful position that the relevant data flows are not subject to the jurisdiction of the Office of the Information & Privacy Commissioner of Alberta because the Personal Information Protection Act (Alberta) ("PIPA") is not constitutionally operative in respect of the transborder data flows involved in this incident. This correspondence is intended to effectively provide your Office with the same information that would be required under PIPA's section 34.1(1) with a view to being as transparent as possible and ensuring your Office is aware of the incident.* In response to the Organization's position, I note that section 3 of PIPA says "The purpose of this Act is to govern the collection, use and disclosure of personal information by organizations …".

	Section 4 says "Except as provided in this Act and subject to the regulations, this Act applies to every organization and in respect of all personal information." [my emphasis] The Organization is an "organization" as defined in section 1(1)(i) of PIPA. PIPA does not contain any territorial or constitutional limitation. I am aware that the *Organizations in the Province of Alberta Exemption Order*, SOR/2004-219 (the Exemption Order) states: > *An organization, other than a federal work, undertaking or business, to which the Personal Information Protection Act, S.A. 2003, c. P-6.5, of the Province of Alberta, applies is exempt from the application of Part 1 of the Personal Information Protection and Electronic Documents Act, in respect of the collection, use and disclosure of personal information that occurs within the Province of Alberta.* The Exemption Order sets out the territorial limitation of the Province of Alberta. With the exception of federal works, undertakings or businesses, organizations that collect, use and disclose personal information within Alberta are exempt from the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA), and PIPA applies. PIPEDA applies to the transborder flow of personal information. However, as provided by the Exemption Order, PIPEDA does not apply to the personal information collected, used or disclosed within Alberta. I do not lose jurisdiction over the collection, use or disclosure of personal information within Alberta just because the personal information subsequently enters a transborder flow. Such an interpretation would result in PIPEDA applying to the collection, use or disclosure of personal information within Alberta, when the Exemption Order says that PIPEDA does not apply. Finally, the Exemption Order is specific only as to the collection, use or disclosure of personal information within Alberta. Consequently, any collection, use or disclosure of personal information within Alberta brings an organization under my jurisdiction, regardless of where the organization may be located. Given the above, it is my view that, to the extent the personal information at issue in this matter was collected by the Organization in Alberta, via a website portal, for example, PIPA applies.

Section 1(1)(k) of PIPA "personal information"	The Organization reported the incident involved some or all of the following information: • name, • email address, • telephone number, • postal address, • date of birth, • emergency contact details, • last four digits of payment card or account number(s) (and expiry date, if applicable), • message threads, • past and future bookings, and • the number of travelers tagged on such bookings, if any. <u>Publicly visible details</u>: • profile photo and/or property photos, • city of residence, • user bio, and • reviews. The Organization also said: *By way of background and as your Office will already be aware, ATOs arise from the use by an Airbnb user of the same password to secure their Airbnb account that they have also used on other sites or apps. When other sites or apps then suffer a security breach, attackers use the credentials they obtain (e.g. email address and password) to attempt to access a variety of platforms on the internet, including Airbnb's platform.* From this, I understand that the malicious actor(s) were able to confirm credentials obtained from sources other than the Organization when they accessed user accounts. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. As noted above, to the extent this information was collected in Alberta, PIPA applies. The Organization reported, "full payment card or account number(s) and government-issued identification documents (if provided) were not visible to the malicious actor." The Organization also reported:

	In some circumstances, the message threads in a user's Airbnb inbox and details in the past and scheduled trip tab may also include third party information, such as a host's contact details and address. Notably, messages are typically logistical in nature (e.g. organizing the accommodation experience such as where to find the keys, things to watch out for, etc.) and contain limited personal information. Where personal information is contained within a message, examples would typically include things like a contact number, clarifying an address (partial or full) of an accommodation or meeting point, or a Wi-Fi password. As such, some of the 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 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." Therefore, I find that PIPA applies to the personal information.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On April 2, 2021, the Organization discovered a technical vulnerability involving user accounts that had been subject to an "account takeover" (ATO). • The Organization reported that the vulnerability did not cause the ATOs; however, it permitted a malicious actor engaged in an ATO to remain logged in to user accounts after the Organization had taken steps to terminate access and force a password reset. • The Organization reported it previously informed its users that their accounts had been accessed and took a series of measures to remove the malicious access to user accounts. However, the issue in the Organization's systems was likely

	introduced on July 17, 2018 in a software upgrade, so the malicious actor may have continued to have access to user accounts and the information in them. • On April 3, 2021, the Organization implemented additional measures to remove the malicious actor's access to user accounts, and restored the accounts. • In the course of an ATO, a malicious actor would have had access to all information that is typically visible to the account user. In some cases, the malicious actor may have made changes to the payment information in user accounts. • The Organization managed to successfully terminate all known ATO account sessions believed to have been affected by the vulnerability.
Affected individuals	The incident affected 170 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Patched the vulnerability. • Terminated all account sessions believed to be affected by the vulnerability. • Reimbursed the vast majority of users who were financially impacted and committed to ensuring that all impacted users are fully reimbursed. • Notified regulatory authorities in Ireland, the UK, Luxembourg, and Canada.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on April 16, 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 reported, *Certain … users have experienced a limited financial loss as a result of a malicious actor making changes to payment details and either redirecting payments away from the user's account to another account associated with the malicious actor (in the case of a host) or scheduling and paying for a fictitious trip (in the case of a guest).* In my view, a reasonable person would consider the contact and identity information at issue could be used for the purposes of identity theft and fraud. Email addresses, particularly in association with the individual's relationship and history with the Organization, could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. Confirmed 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 provide an assessment of the likelihood that significant harm would result from this incident; however, depending on the specific situation, its notification to affected individuals said, <u>Notification 1</u> *While we have no reason to believe at this time that your information was actually misused, we wanted to notify you out of an abundance of caution. We recommend that you remain vigilant for any signs of suspicious activity on your Airbnb account, and alert us immediately if such activity occurs. We also encourage you to review these tips about how you can help keep your account and information secure: How can I keep my account secure?* <u>Notification 2</u> *While we have no evidence to suggest that any unauthorized monetary transactions actually occurred as a result of this incident, we wanted to alert you of the situation out of an abundance of caution and to ensure that you've reviewed your account thoroughly, including all payment methods and payout methods listed in your account. If you suspect any suspicious activity on your account, please contact us as soon as possible, and we will work to correct any unauthorized activity. We also encourage you to review these tips about how you can help keep your account and information secure: How can I keep my account secure?* *<u>Notification 3</u>* *After this discovery, our team implemented additional measures on April 3, 2021 to remove the individual's access to your account and restored your account. We do, however, suspect that the unauthorized user may have successfully diverted funds or made unauthorized transactions on your account. To the extent this occurred, we have already reimbursed you directly or via your payment or payout method. If you suspect any additional irregularities in your account, please contact us as soon as possible, so that we can assist you. We encourage you to review your account thoroughly, including all payment methods and payout methods in your account, along with this information on how to keep your account secure: How can I keep my account secure?* In my view, a reasonable person would consider the risk of harm is increased as the incident was the result of malicious intent

	(deliberate account take overs). The Organization reported that credentials were used to access user accounts illegally and without authorization and, in some cases, to divert funds and make unauthorized transactions. It appears the malicious actor(s) may have continued to have access to user accounts and the personal information in them for approximately 2 ½ years before the Organization discovered the threat.

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 identity information at issue could be used for the purposes of identity theft and fraud. Email addresses, particularly in association with the individual's relationship and history with the Organization, could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. Confirmed credentials could be used to compromise other online accounts. These are significant harms.

The risk of harm is increased as the incident was the result of malicious intent (deliberate account take overs). The Organization reported that credentials were used to access user accounts illegally and without authorization and, in some cases, to divert funds and make unauthorized transactions. It appears the malicious actor(s) may have continued to have access to user accounts and the personal information in them for approximately 2 ½ years before the Organization discovered the threat.

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 the affected individuals by email on April 16, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner