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 (the "Organization" or "Airbnb")
Decision number (file number)	P2021-ND-279 (File #017582)
Date notice received by OIPC	October 2, 2020
Date Organization last provided information	October 21, 2020
Date of decision	February 17, 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 providing the information set out below on a courtesy basis, however, 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." In an October 21, 2020 email, the Organization clarified: *Airbnb respectfully maintains the position that PIPA is not constitutionally operative in respect of the transborder data flows involved in this incident, but its correspondence of October 2, 2020 was intended to effectively provide your Office with the same information that would be required under section 34.1, with a view to being as transparent as possible and ensuring your Office was aware of the incident. Hence assuming, though not conceding, that your Office does have jurisdiction in transborder situations such as this one, you will have received de facto notification of the information required. Airbnb has asked us to reiterate that it fully intends to continue working with your Office to*

	provide material updates, respond to queries, and cooperate in responding to any questions your Office may have with respect to this matter. 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, PIPA applies.
Section 1(1)(k) of PIPA "personal information"	The incident involved some or all of the following information: <u>For most of the affected individuals:</u> • name, • contact number (mobile and landline telephone number), • partial or full address, • meeting point, • wifi password, and • logistical information (e.g. organizing the accommodation experience, where to find keys, things to watch out for, etc.) <u>For one Alberta resident using the Organization's business product "Airbnb for Work":</u> • name, • work email, and • profile photo. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The personal information at issue was collected via either mobile apps or the Organization's website. To the extent this information was collected in Alberta, PIPA applies. The Organization reported that, of the affected individuals in Alberta, "seven were individuals and seven were corporate contacts (i.e. representatives of businesses)." 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 September 24, 2020, the Organization discovered a technical issue that caused the incorrect messaging inbox to be displayed to certain users for a short period of time (i.e. three hours). During this time, users might have inadvertently accessed the messages of other users when attempting to use their own inbox. • The Organization investigated and found that a defect in its content delivery network (CDN) caused certain users' API requests to be cached incorrectly. The error was introduced into the Organization's caching logic through configuration prepared by a third-party service provider.
Affected individuals	The incident affected 243 individuals residing in Alberta. The Organization reported, "there are two classes of affected individuals. The first (almost all affected individuals) involves individuals where the incorrect messaging inbox may have been temporarily displayed...The second class (involving a single Alberta resident) involves individuals where the incorrect Airbnb for Work dashboard or account settings may have temporarily displayed."
Steps taken to reduce risk of harm to individuals	• Investigated the incident. • Contained and corrected the error. • Exploring steps with its CDN service provider to help prevent a similar occurrence and considering several internal control enhancements.
Steps taken to notify individuals of the incident	Affected individuals were notified on October 12 and October 13, 2020.

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 possible harms that might result from this incident; however, its notification to affected individuals said "We have no reason to believe that any of your messages were improperly used or any other account information was exposed, but we wanted to make you aware of this issue out of an abundance of caution." The Organization's notification to the Alberta resident affected in connection with Airbnb for Work also said "please be alert to requests for information sent to your work email address out of an abundance of caution." In my view, a reasonable person would consider the contact and email addresses or mobile telephone numbers could be used for the purposes of smishing/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 reported, *Given the limited nature of the personal information involved, the fact that in many instances there will be limited personal information in the messages exposed, the limited time period during which the data was exposed (i.e. approximately 3 hours) and was only seen by another authenticated user, all of whom Airbnb regards as trusted members of the Airbnb community, Airbnb believes that the risk of harm to impacted individuals is low.* In my view, a reasonable person would consider that the likelihood of harm is reduced because the breach did not result from malicious intent. I also accept the Organization's assertion that in each case, the data was only seen by another authenticated user within the Airbnb community. However, it is not clear from the Organization's report how many individuals may have accessed the information or whether it confirmed that the users who inadvertently accessed the messages of other users did not use, make copies, further disclose, or otherwise distribute the personal information they may have been able to view.
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 email addresses or mobile telephone numbers could be used for the purposes of smishing/phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are significant harms. The likelihood of harm is reduced because the	

breach did not result from malicious intent. I also accept the Organization's assertion that in each case, the data was only seen by another authenticated user within the Airbnb community. However, it is not clear from the Organization's report how many individuals may have accessed the information or whether it confirmed that the users who inadvertently accessed the messages of other users did not use, make copies, further disclose, or otherwise distribute the personal information they may have been able to view.

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 on October 12 and October 13, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner