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	American Councils for International Education ("Organization")
Decision number (file number)	P2022-ND-075 (File #023183)
Date notice received by OIPC	September 15, 2021
Date Organization last provided information	September 15, 2021
Date of decision	January 10, 2023
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's head office is in Washington, DC. 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 some or all of the following information: • name, • contact details, • education records, • medical records, • mental health records, • requests for accommodations (physical, health, visual, learning), • insurance information, • passport and visa records. • ethnicity, • data on religious beliefs, • health data, and • criminal history data. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.

DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• On April 28, 2021, the Organization became aware that a limited number of finalists in one of its programs received administrator-level viewing access to the web-based database it uses to collect and maintain records for applicants, finalists and participants in the programs it administers. • The Organization determined that personal records were among those that were accessible, although the Organization have not determined what records have been viewed.
Affected individuals	The incident affected 416 individuals including 5 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Terminated all access to the database. • Provided the correct access to the finalists, and again enabled their access to the database (with the correct access). • Undertook an internal investigation to attempt to determine whether any unauthorized access to information occurred, the possible causes for the data exposure and measures it could take to ensure that a similar situation would not occur in the future. • Revising user profiles so that user access is the default access and ensuring that applicants, finalists and participants cannot be given administrator-level access. • Conducting refresher training for all personnel who administer the database.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on April 28, 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, *Among the categories of personal data that were exposed in the data breach were data on ethnicity, data on religious beliefs, health data and criminal history data. Unauthorized use of these categories of personal data could have a significant negative impact on the rights and freedoms of natural persons as assumptions can be made about a person's health, intellectual abilities, financial status and criminal status. This in turn could lead to discrimination, financial distress and identity fraud.*

	In my view, a reasonable person would consider the contact and identity information could be used for the purposes or identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. Medical records, accommodation records and criminal history data could be used for the purposes of hurt, humiliation, embarrassment or damage to reputation. Ethnicity and religious beliefs could be used to cause discrimination. These are all 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, *So far there has been no indication that any personal data was misused... Of the 550 program finalists who received administrator-level view access, only 375 accessed the database during the period they had that access. They were able to view the current and past applicant, finalist and participant records going back to 2009 for approximately 416 Canadian data subjects maintained in the database, although American Councils has not been able to determine and will not be able to determine whether they did view any other individual's records.* *It is important to note that participant files and data are randomized in the AIS Forms database. During the limited exposure, a person viewing the data could not search, filter, or organize the files in question and participants were not grouped by program or last name. At no time did any of the finalists have the ability to edit any records in the database other than their own. Also, none of the finalists had access to any recommendations or application evaluations for any participants.* *In addition, none of the finalists had access to any credit card information because American Councils does not collect payment information in the AIS Forms database. Information about participation in a program such as locations of programs and dates of program participation and travel was not available. Please also note that the data that was exposed is stored in the application intake portal, not the program management system. For these reasons, we remain confident that the risk of any misuse of these records is extremely 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 other authenticated users within Organization's community. However, the Organization was

	not able to determine what records have been viewed. A known, unintended recipient notified the Organization of the incident but it is not clear from the Organization's report whether it confirmed that the users who inadvertently accessed the information at issue did not use, make copies, further disclose, or otherwise distribute the personal information they may have been able to view. Finally, it is not clear whether there are known personal or professional relationships between the unintended recipients and the affected individuals, which, increases the likelihood that embarrassment, hurt, humiliation and damage to reputation could result.

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.

Contact and identity information could be used for the purposes or identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. Medical records, accommodation records and criminal history data could be used for the purposes of hurt, humiliation, embarrassment or damage to reputation. Ethnicity and religious beliefs could be used to cause discrimination. These are all 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 other authenticated users within Organization's community. However, the Organization was not able to determine what records have been viewed. A known, unintended recipient notified the Organization of the incident but it is not clear from the Organization's report whether it confirmed that the users who inadvertently accessed the information at issue did not use, make copies, further disclose, or otherwise distribute the personal information they may have been able to view. Finally, it is not clear whether there are known personal or professional relationships between the unintended recipients and the affected individuals, which, increases the likelihood that embarrassment, hurt, humiliation and damage to reputation could result.

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 letter of April 28, 2021 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance