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	The Japan Foundation- Toronto (Organization)
Decision number (file number)	P2019-ND-080 (File #009940)
Date notice received by OIPC	October 4, 2018
Date Organization last provided information	May 15, 2019
Date of decision	June 24, 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 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 is located in Toronto, Ontario. The Organization operates on a not-for-profit basis, but is not a "non-profit" organization as defined in PIPA, such that it would only be subject to PIPA in relation to personal information collected, used and disclosed in connection with a commercial activity. 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: • name, • email address, • date of birth, and • gender. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected via the Organization's website.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	

Description of incident	• On September 30, 2018, the Organization's third-party website developer failed to save a portion of the back-end of the website as viewable by "admin only", such that the page and a link were viewable by the public. • At the time of the breach, there were 200 fake names included for the purpose of testing, but the list also included people who signed up for the test September 28, 2018. • The Organization's staff discovered the incident on October 1, 2018 after checking the website.
Affected individuals	The incident affected 4 (four) individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Removed the link from the main page and adjusted the settings on the site so that personal information is only viewable by authorized administrative. • Ensuring that personal data is kept hidden from the public and added an SSL certification to the page.
Steps taken to notify individuals of the incident	The affected individuals were notified in writing on October 4, 2018.
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 "There is a possibility that unknown third parties could have accessed the personal information. Based on the nature of the information, risks could include phishing attempts or fraud." I agree with the Organization's assessment. A reasonable person would consider that the identity information at issue in this case could be used to cause the harms of identity theft and fraud. Email addresses 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 reported that it believes "… the liklihood [sic] of harm is low, as the incident was due to a technical error and there is no … evidence the information was accessed by anyone with malicious intent. Also, according to our third-party website developer, there were only 28 page views while it was public (of which their investigation to-date indicates that approximately 15 were the developers access the site, 2-6 were repeated views by the same user, and 2-3 were the server cache updating copies of the site). The website has low traffic and is hosted behind a Cloudflare account for security reasons, so no additional information beyond what was displayed could be accessed. In our view, the risks are reduced by the fact that only a small number of unauthorized persons access the site."

	In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is decreased as the breach resulted from human error and not malicious intent. However, the information may have been exposed for a couple of days. Although the Organization said that there is no evidence the information was accessed by anyone with malicious intent, it cannot be certain as the information was accessed by a "small number of unauthorized persons" and phishing, identity theft and fraud can occur months and even years after a data breach.

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 identity information at issue in this case could be used to cause the harms of identity theft and fraud. Email addresses 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 decreased as the breach resulted from human error and not malicious intent. However, the information may have been exposed for a couple of days. Although the Organization said that there is no evidence the information was accessed by anyone with malicious intent, it cannot be certain as the information was accessed by a "small number of unauthorized persons" and phishing, identity theft and fraud can occur months and even years after a data breach.

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 in writing on October 4, 2018 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner