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	Zoosk Inc. (Organization)
Decision number (file number)	P2020-ND-091 (File #016122)
Date notice received by OIPC	June 10, 2020
Date Organization last provided information	August 31, 2020
Date of decision	September 1, 2020
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 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 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, • username (email address), • account password, • date of birth, • generalized demographic information, • gender search preferences, and • religious or political preferences. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The personal information was collected via the Organization's website. To the extent that personal information was collected in Alberta, I have jurisdiction in this matter.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On May 11, 2020, an unknown third party claimed to have accessed certain personal information of members of the Organization. • Based on its investigation, the Organization learned that on or about January 12, 2020, an unauthorized third party gained access to the Organization's data stored in a database hosted by a third party. • The Organization learned that although a copy of the database is available online the decipher key is not, and therefore most of the more sensitive data was not compromised. • The database did not contain financial or credit card data. • The Organization reported that it routinely anonymized a number of data fields in the database at issue so that user responses were typically not readable in plain text.
Affected individuals	The incident affected 24.2 million individuals, of which 1,140,431 were Canadian. The Organization reported that it maintains email address information for its members but not physical address information. Accordingly, the number of Alberta residents affected is unknown.
Steps taken to reduce risk of harm to individuals	• Commenced an investigation. • Contacted law enforcement authorities. • Notified affected individuals. • Notified the Federal, BC and AB Privacy Commissioners. • Taking steps to monitor systems and enhance security measures and processes.
Steps taken to notify individuals of the incident	Affected individuals were notified by email between June 3, 2020 and June 10, 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 reported it "…considers the affected information to present a low risk of harm, particularly since profile information is typically disclosed among … users and passwords can be easily changed, although there is a potential risk of phishing". In my view, a reasonable person would consider the contact (name, demographics), credential (username and password) and identity (date of birth) information at issue 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 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 did not specifically provide an assessment of the likelihood that significant harm would result from this incident. However, in its notice to affected individuals it said, *We ask that you consider taking some protective measures as well. Out of an abundance of caution, we encourage you to change your …password. Regularly rotating online passwords is a good security practice, as is avoiding the use of the same or similar passwords on multiple sites; consider selecting complex passwords with upper and lower case and special characters. You may also consider using a password generator from a trusted password tool. In addition, it is always a good idea to remain vigilant against threats of identity theft or fraud and to regularly review and monitor your accounts and credit history for any signs of unauthorized transactions or activity. If you ever suspect that you are the victim of identity theft or fraud, you have the right to file a report with the police or law enforcement. Finally, please be alert to "phishing" emails from someone who acts like they know you and requests sensitive information over email, such as passwords, financial information or government identification numbers* In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). Further, the information may have been exposed for approximately four months.

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 (name, demographics), credential (username and password) and identity (date of birth) information at issue 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 all significant harms.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). Further, the information may have been exposed for approximately four months.

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 between June 3, 2020 and June 10, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner