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	eHarmony, Inc. (Organization)
Decision number (file number)	P2019-ND-167 (File #013328)
Date notice received by OIPC	June 3, 2019
Date Organization last provided information	June 3, 2019
Date of decision	November 20, 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 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, • contact information, • username, • password, • limited payment card data (excluding free subscriptions), • preferences in matches, • matches, • location data (limited to city, province and country), • subscription status, and • if shared, ethnicity, religion, and political opinion. Payment card data within an account is limited to the last 4 digits of a user's credit card only: it does not include CVV, expiration date nor the full card number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On May 21, 2019 an analyst with the Organization was monitoring social media and found a YouTube video that had been uploaded by an unknown third party and which displayed a list of the Organization's accounts. In the YouTube video, the third party is seen to be advertising a software tool that is used to test lists of user account credentials, in order to identify accounts susceptible to being compromised. • The Organization commenced an internal investigation and found that an attacker appeared to have directed valid and invalid credentials (not obtained from the Organization) at the Organization's systems in order to determine which credentials worked and which did not. Specifically, on or around May 21, 2019, there were 482,000 attempts by the unauthorized third party to access the Organization's accounts using these credentials. Most attempts were blocked or denied; however, some credentials were valid and enabled the unauthorized party to access user accounts illegally and without the user's authorization.
Affected individuals	The incident affected three (3) individuals in Alberta.
Steps taken to reduce risk of harm to individuals	• Submitted takedown requests in respect of the posted content (e.g. on YouTube). • Required a password reset for affected accounts to ensure that compromised passwords cannot be used again. • Implemented an automatic password reset if a customer had not logged in for 12 months.
Steps taken to notify individuals of the incident	Affected individuals received an email notification on May 21 and 22, 2019. A follow-up email was sent on June 3, 2019.
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 the potential harms that might result from this incident, but its June 3, 2019 notice to affected individuals said "It is possible that your account may have been accessed and any information including your profile information available through your account could have been seen and used by the third party with the intention of causing you harm (e.g. identity theft)." In my view, a reasonable person would consider the contact, credentials and profile information at issue could be used to cause the significant harms of identity theft and fraud -- particularly if the

	contact information included email addresses -- and could be used to compromise other online accounts. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud.
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 assess the likelihood of harm resulting from this incident but said, with respect to the possibility of the third party using the information to cause harm to affected individuals: "Although we have no reason to believe that this is the case, we advise you to be extra vigilant in monitoring any suspicious activities relating your account or your accounts with other online services. To help keep your account safe, we also recommend that you change your password frequently and not use the same password on different services." In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the personal information was compromised due to deliberate action by an unknown party, using compromised credentials.

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, credentials and profile information at issue could be used to cause the significant harms of identity theft and fraud -- particularly if the contact information included email addresses -- and could be used to compromise other online accounts. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to deliberate action by an unknown party, using compromised credentials.

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 affected individuals received an email notification on May 21 and 22, 2019. A follow-up email was sent on June 3, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner