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	ZipRecruiter Inc. (Organization)
Decision number (file number)	P2020-ND-106 (File #014919)
Date notice received by OIPC	January 17, 2020
Date Organization last provided information	June 24, 2020
Date of decision	September 24, 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 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, • email address, • telephone number, • city, • state, • location of job, • date of application, • date application was viewed by client-user, • CV and resume (work experience, years of experience, industry, desired salary, executive summary, educational qualifications, education institution, career/job objectives, achievements, licenses or certifications, associations, skills, references), • responses to questions posed by the client-user, • veterans status, and • designated website profiles in client-user's account (e.g., Twitter profile, LinkedIn profile, Facebook.

	This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization provides a website, which enables job seekers to search for employment opportunities and client-users to source candidates by posting job openings on the website and/or by searching a CV/resume database. • On December 13, 2019, the Organization was notified that a job seeker reported receiving an unsolicited email that appeared to come from a client-user account and requested she send her resume to a third party email address not associated with the client. • The Organization investigated and discovered that the unique login credentials of 30 client-user accounts had been compromised. • The Organization contacted affected client-users to obtain information concerning how the login credentials may have been or were compromised. To date, the Organization has not received any material response or relevant information from these client-users.
Affected individuals	The incident affected 581 Canadians. The Organization reported that it is not possible to ascertain whether Alberta residents have been affected by this incident.
Steps taken to reduce risk of harm to individuals	• Reset passwords on all affected client-user accounts. • Deactivated any additional accounts created by the unauthorized individual(s). • Notified affected (legitimate) client-users. • Made changes to the Verification Email Feature after discovering the unauthorized access.
Steps taken to notify individuals of the incident	All Canadian-based job seekers who may have been affected by the incident were notified by email on January 16, 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	The Organization did not specifically identify any harm that might result from this incident, but its notification to affected individuals stated: *Although we are not certain of the purpose of the unauthorised access, the unauthorised access to your*

important, meaningful, and with non-trivial consequences or effects.	*personal information could be utilised to send you spam or phishing emails. A phishing email is used by cyber-criminals to obtain sensitive information by tricking the recipient into clicking malicious links, downloading attachments, or sending personal, financial or other sensitive information. Phishing emails tend to impersonate well know companies or brands, or even people you work with or your friends. Their goal is to present the sender of the email in a manner that puts the recipient off his or her guard.* The Organization also provided information in its notification to affected individuals on how to protect themselves against fraud. In my view, a reasonable person would consider the contact, identity and resume information at issue could be used to cause the harms of identity theft and fraud. Email address, particularly when combined with other personal information, 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 provide an assessment of the likelihood that significant harm would result from this incident. In my view, a reasonable person would consider the likelihood of harm resulting in this case is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion) who gained access to at least one job seeker's email address. The Organization reported that it is not possible to know how long accounts may have been compromised.

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, identity and resume information at issue could be used to cause the harms of identity theft and fraud. Email address, particularly when combined with other personal information, could be used for phishing purposes, increasing vulnerability to identity theft and fraud. The likelihood of harm resulting in this case is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion) who gained access to at least one job seeker's email address. The Organization reported that it is not possible to know how long accounts may have been compromised.

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 on January 16, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner