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	Entrust Disability Services, as reported by Box Clever (the Organization)
Decision number (file number)	P2019-ND-093 (File #012096)
Date notice received by OIPC	February 21, 2019
Date Organization last provided information	February 21, 2019
Date of decision	June 27, 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 an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The Organization reported the incident involved "Resumes", including the following personal information: • "Address, phone, and email addresses" • "Employment history" 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	The Organization is a web design company. The Organization reported the following with respect to the website www.entrustdisabilityservices.ca: *Issue #1: Directory Access* *Upon investigation of the issue, it was determined that between December 27, 2018 and January 11, 2019 a server misconfiguration allowed for directories on websites to be indexed. This created the potential for certain files to be*

	accessed that should not have been. When this misconfiguration was discovered on January 11 it was fixed immediately. The folder that was made accessible was called "/public" and its purpose is to hold files needed to render websites, such as images, Javascript, and CSS files. Our initial assessment of the impact of the misconfiguration was that it posed a minimal risk. *Issue #2: File Storage Locations* *On January 14, a second issue was discovered; a bug in the code that was incorrectly storing certain files in a sub-folder of "/public".* *Issue #3: Search Engine Indexes* *The combination of storing these files in an incorrect location and then allowing that location to be accessed may have resulted in access to these files. The probability of people discovering these files was extremely low. Our primary concern is with automated crawlers, bots, and search engines discovering the files, and then subsequent access by human visitors via search results.*
Affected individuals	The Organization did not report the number of affected individuals.
Steps taken to reduce risk of harm to individuals	• Disabled access to any affected websites while working to implement a solution. • Patch was put in place and website service was restored to those affected. • Checked with major search engines to see if any data was indexed or cached. None was discovered. • Directory Access was fixed on January 11 by reconfiguring the affected servers. • File Storage Locations was fixed on January 14 with a change to the code that handles file storage. • Search Engine Indexes was addressed on January 14 and 15. The Organization submitted removal requests to Google for websites that were determined to be affected. • A code audit on websites is underway to ensure similar bugs do not exist elsewhere. • An internal post-incident review will occur to take action on preventing future incidents of this nature.
Steps taken to notify individuals of the incident	The affected individual(s) have not been notified.

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 the following possible harms: *1. Address, phone, and email addresses could have been accessed by third parties.* *2. Employment history of an individual could have been accessed by third parties.* *3. Employers could potentially become aware of an employee applying for work elsewhere.* In my view, a reasonable person would consider that the contact and employment information, as well as education history typically included on a resume, could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing affected individuals' vulnerability to identity theft and fraud. The Organization also noted that "Employers could potentially become aware of an employee applying for work elsewhere", which could result in loss of employment or embarrassment. 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: *The likelihood of harm is unlikely, given that we believe, with a high degree of certainty, no data was accessed.* *If the data had been accessed, the likelyhood [sic] of harm is low. Depending on an individual's current employment status or contract, there could be harm to their employment with the current employer discovered their application.* *The likelihood of fraud or other harm from address and contact information being accessed is also low.* The Organization also said: "NOTE: No breach actually occurred. There was a security lapse on the servers hosting the website that may have resulted in access to resumes of job applicants to this website. This report is proactive at the recommndation [sic] of the OIPC." In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is decreased as the breach did not result from malicious intent. However, the information was potentially exposed for over two weeks. Despite the fact the Organization reported that it "…believe[s], with a high degree of certainty, no data was accessed", the Organization did not provide any information to support why it believes this to be true (e.g. are there audit logs demonstrating that there was no access?).

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 contact and employment information, as well as education history typically included on a resume, could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing affected individuals' vulnerability to identity theft and fraud. The Organization also noted that "Employers could potentially become aware of an employee applying for work elsewhere", which could result in loss of employment or embarrassment. These are all significant harms. The likelihood of harm resulting from this incident is decreased as the breach did not result from malicious intent. However, the information was potentially exposed for over two weeks. Despite the fact the Organization reported that it "…believe[s], with a high degree of certainty, no data was accessed", the Organization did not provide any information to support why it believes this to be true (e.g. are there audit logs demonstrating that there was no access?). **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) and confirm to my office, in writing, within 10 days of the date of this decision, that it has done so.**

Jill Clayton
Information and Privacy Commissioner