

RECEIVED
APR 08 2019
CONSUMER PROTECTION

April 3, 2019

VIA CERTIFIED MAIL

Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Jobscience Data Breach Notification

Dear Sir or Madam,

I am writing to inform your office of a data breach experienced by my client, Jobscience, Inc. (“**Jobscience**” or the “**Company**”), a Bullhorn, Inc. company (“**Bullhorn**”).

Jobscience offers a software platform product that its customers utilize to streamline their hiring processes and manage information submitted by job applicants. In March 2018, Bullhorn acquired Jobscience.

Jobscience was informed by agents from the Federal Bureau of Investigation (FBI) in August 2018 that the agents had observed certain data being exfiltrated from a Jobscience server. After the FBI provided Jobscience a copy of the data on August 21, 2018, Jobscience confirmed that the data did, in fact, come from a Jobscience server. Subsequent investigation determined that a legacy Jobscience TalentPath server that housed information related to individuals who had applied for positions with Jobscience customers was accessed by an unauthorized third party, who then exfiltrated the data housed on the server (the “**Attack**”). While certain information in the server was encrypted at rest, the results of the investigation suggest that the unauthorized party may have had sufficient access as to be able to exfiltrate the decryption mechanism. No other elements of the Jobscience environment are believed to be involved in the Attack.

Jobscience took prompt action upon confirming that the data came from its server. Specifically:

- Jobscience initiated an investigation to identify (i) the root cause of the Attack and (ii) the nature and scope of the compromised data. To aid in its investigation, Jobscience retained outside

forensic auditors to conduct an independent review of the details surrounding the incident and the data involved.

- Jobscience notified all customers that had information in the implicated server about the Attack on August 28, 2018, via letter and telephone, and thereafter provided each customer with details about their implicated data.
- After an initial investigation identified the potential vulnerability used in the Attack, Jobscience took steps to resolve the vulnerability by (i) deploying a patched version of the server and migrating all of its customers to the patched server, and (ii) updating user credentials by forcing all administrators and users to update their passwords.
- Jobscience retained a database consultant to analyze the data exfiltrated in the Attack to identify affected records and the customers to which those records belonged. In September 2018, Jobscience provided to those customers detailed information regarding the affected records that Jobscience had identified as belonging to the customer, to assist the customers with any applicable notification obligations.¹ Further analysis of the database identified additional records belonging to these customers that was implicated in the Attack, and Jobscience intends to supplement our previous reports to those customers with this new information.

In addition, this further analysis of the database identified two new categories of implicated records: (i) records that relate to Jobscience's historic use of the platform for its own hiring and applicant management processes; and (ii) records that are not readily attributable to any particular Jobscience customer. Jobscience is providing notice to individuals whose information falls into these two categories, as well as to individuals whose records belong to a customer but who have not been previously notified (unless the customer affirmatively tells Jobscience that it wants to perform the notification). Jobscience is providing this notice to you because our records indicate that 501 individuals that Jobscience intends to notify are residents of New Hampshire.

Jobscience plans to send notification to affected residents on April 4, 2019. Jobscience is also notifying residents of New Hampshire via the substitute notice mechanism, due to the lack of sufficient contact information in some records. Specifically, Jobscience plans to post to its website a notice about the Attack, plans to issue a press release, and plans to send an email notice to those individuals for whom Jobscience has relevant contact information.

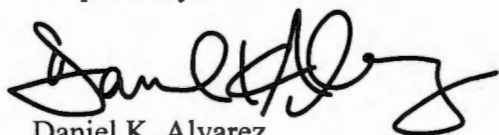
Jobscience will be offering identity theft protection, including credit monitoring services, for 12 months to all notified individuals at no cost to them.

¹ As a result, your office may have previously received notice of this incident from one or more of our customers acting pursuant to their notification obligations.

Office of the Attorney General
April 3, 2019
Page 3 of 3

If you have any questions, please do not hesitate to contact me at dalvarez@willkie.com or 202-303-1125.

Respectfully,

A handwritten signature in black ink, appearing to read "Daniel K. Alvarez", written in a cursive style.

Daniel K. Alvarez