WILLKIE FARR & GALLAGHER LLP

1875 K Street, N.W.
Washington, DC 20006-1238

Tel: 202 303 1000
Fax: 202 303 2000

July 12, 2019

VIA EMAIL

Security Breach Notifications
Consumer Protection Division
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106

Re: Jobscience Data Breach Notification

To Whom It May Concern,

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 with 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 exploited 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 each customer in order to assist those customers with any applicable notification obligations.[1] Further analysis of the database identified additional records belonging to these customers that were implicated in the Attack, and Jobscience has supplemented its previous reports to those customers with this new information.

This further analysis identified two new categories of implicated records: (i) records that related to Jobscience's historic use of the platform for its own hiring and applicant management processes; and (ii) records that were not readily attributable to any particular Jobscience customer. Jobscience has provided 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 told Jobscience that it wanted to perform the notification itself).

I am submitting this notification on behalf of Jobscience because, as part of the process described above, Jobscience just recently identified a sufficient number of Iowa residents affected by the Attack to cross the 500-resident threshold for notification to your office as set forth in Iowa Code Chapter 715C. Specifically, Jobscience sent notifications to 449 affected Iowa residents on April 4, 2019. Subsequently, working with its customers, Jobscience identified an additional 89 affected Iowa residents that needed to be notified, and notified them on July 9, 2019. As such, Jobscience notified a total of 538 affected Iowa residents. Sample copies of those notifications are attached to this letter.

---

[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.

Jobscience has also notified affected individuals via substitute notice, due to the lack of sufficient contact information in some records. These records may include some residents of Iowa. Specifically, Jobscience has posted to its website a notice about the Attack, has issued a press release, and has sent 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.

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

Respectfully,

Daniel K. Alvarez

Attachments

[DATE]

[Name]
[Address]
[City, State Zip Code]

Re: Notice of Data Breach

Dear [First Name],

I am writing to inform you that Jobscience, Inc.'s ("Jobscience") TalentPath product experienced a cyberattack that resulted in unauthorized third-party access to certain TalentPath users' personal information. Jobscience takes the security and integrity of the data entrusted to us very seriously. As described below, we have taken steps to protect your information from further unauthorized disclosure, and we are providing certain information and services to help you protect yourself.

WHAT HAPPENED

We learned in late August 2018 that an unauthorized third-party may have gained access to one of our servers on or around May 8, 2018. We conducted a comprehensive investigation of the incident, and determined that the unauthorized third party was able to gain access to a single server used to process job application information, including information you likely submitted when you applied for a position with a Jobscience customer. Law enforcement is aware of the incident, but this notification was not delayed as a result of a law enforcement investigation.

You may have previously received a letter from a Jobscience customer regarding this incident. One of the first things Jobscience did after it discovered the attack was to notify our customers so they could reach out to affected individuals. Several customers used information Jobscience provided to notify affected individuals about the incident based on available information. Further investigation revealed that additional personal information may have been accessed in the attack, which is the reason for this letter.

WHAT INFORMATION WAS INVOLVED

The affected data generally includes information submitted by or on behalf of job applicants, such as names and contact information, and in some instances information such as Social Security Number, date of birth, Driver's License Number, Alien Registration Number, username, password or security question. The information may have been submitted by or through your employer or a recruiter or staffing service who utilized the TalentPath service.

WHAT WE ARE DOING

We have already taken steps to address this incident and protect your personal information from further unauthorized disclosure. In particular, we have remedied the underlying cause of the unauthorized access by deploying patches to the server that was accessed, and we have forced a password reset for all accounts so that the attacker cannot use any information gleaned from the attack to gain further entry to the server. The security and confidentiality of the data we process is one of our top priorities, and we will continue to examine ways we can better protect your data.

WHAT YOU CAN DO

We are enclosing a tip sheet that contains information about how to obtain copies of your credit reports (including tips for doing so free of charge), which you should review for any unexplained activity, and information about how to set up fraud alerts or security freezes on your accounts (which are also offered free of charge). A fraud alert lasts for 1 year. You can simply call one of the three credit reporting agencies at the number in the attached tip sheet. A security freeze prohibits a credit reporting agency from releasing any information from your credit report without written authorization. Please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. To place a security freeze on your credit report, you should contact **each** of the three major consumer reporting agencies (Equifax, Experian, and TransUnion) using one of the contact methods provided on the enclosed tip sheet.

Additionally, we advise you to take the time to change the passwords and security questions and answers you use for any of your online accounts, particularly accounts for which you may have used the same username and password as you used for your Jobscience account (if applicable).

CREDIT MONITORING SERVICE

To help protect your identity, we are offering a complimentary one-year membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **September 30, 2019** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/credit
- Provide your **activation code**: **[code]**

A credit card is **not** required for enrollment in Experian IdentityWorks. If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-890-9332 by **September 30, 2019.** Be prepared to provide engagement number **DB13346** as proof of eligibility for the identity restoration services by Experian.

You can contact Experian **immediately** regarding any fraud issues. If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 1-877-890-9332. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, Experian has Identity Restoration agents available to work with you to investigate and resolve each incident of fraud that occurred.

We encourage you to remain vigilant over the coming months and regularly review your bank and other financial account statements, as well as your credit report. If you have any reason to believe you may be the victim of identity theft, or notice any suspicious activity on any of your accounts, the attached tip sheet contains a number of important steps you should take, including immediately notifying the relevant institution, your local law enforcement agency, your state's Attorney General, and the Federal Trade Commission.

FOR MORE INFORMATION

For more information or should you have any questions, please visit https://talentpath.jobscience.com/.

Sincerely,

Bill Knox
Director Security
Jobscience, Inc.

TIP SHEET OF HELPFUL INFORMATION

REVIEW YOUR CREDIT REPORTS

To obtain an annual free copy of your credit reports, visit www.annualcreditreport.com or call 1-877-FACT ACT. You may also contact the major credit reporting agencies directly:

- Equifax: 1-800-685-1111; P.O. Box 740241, Atlanta, GA 30374; www.equifax.com
- Experian: 1-888-397-3742; 475 Anton Blvd. Costa Mesa, CA 92626; www.experian.com
- TransUnion: 1-800-888-4213; 2 Baldwin Place, P.O. Box 2000, Chester, PA 19022; www.transunion.com

Once you receive your reports, review them carefully for inquiries from companies you did not contact, accounts you did not open, or debts you cannot explain. Verify the accuracy of your Social Security number, address(es), complete name, and employer(s). If any information is incorrect or you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

CONSIDER A FRAUD ALERT AND/OR SECURITY FREEZE

Consider contacting the fraud department of at least one of the three major credit reporting agencies to request that a "fraud alert" and/or "security freeze" be placed on your file, and include a statement that creditors must get your permission before any new accounts are opened in your name. To place a security freeze on your file, you should contact **each** of these agencies using the contact information below, but you only need to contact one of the three credit bureaus to place a fraud alert:

- Equifax
  - Fraud Alert: Visit https://www.alerts.equifax.com or call 1-800-525-6285.
  - Security Freeze: Visit https://www.freeze.equifax.com, call 1-800-349-9960, or send a written request to Equifax Security Freeze, P.O. Box 105788, Atlanta, GA 30348.
- Experian
  - Fraud Alert: Visit https://www.experian.com/fraud or call 1-888-397-3742.
  - Security Freeze: Visit https://www.experian.com/freeze, call 1-888-397-3742, or send a written request to Experian Security Freeze, P.O. Box 9554, Allen, TX 75013.
- TransUnion
  - Fraud Alert: Visit https://fraud.transunion.com or call 1-800-680-7289.
  - Security Freeze: Visit https://freeze.transunion.com, call 1-888-909-8872, or send a written request to TransUnion Security Freeze, Fraud Victim Assistance Department, P.O. Box 6790, Fullerton, CA 92834.

SUGGESTIONS IF YOU SUSPECT YOU ARE A VICTIM OF IDENTITY THEFT

- **Contact the U.S. Federal Trade Commission ("FTC")**. The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. File a report with the FTC or get more information about steps to consider taking by visiting www.identitytheft.gov; calling the FTC's Identity Theft Hotline: 1-877-IDTHEFT (438-4338); or sending a written request to Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, DC 20580. You can find additional information about identity theft from the FTC by visiting www.consumer.gov/idtheft.
- **Filing and obtaining a U.S. police report**. In some states, you have a right to file a police report and get a copy of the report from your local police department or sheriff's office. You should also consider notifying your state's Attorney General. You can find contact information at https://www.usa.gov/state-attorney-general. Some creditors and others may require proof of a crime in order to clear up your records.
- **Keep a record of your contacts**. Start a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.