Davis Wright Tremaine LLP

Suite 800
1919 Pennsylvania Avenue N.W.
Washington, D.C. 20006-3401

Christin McMeley
202-973-4264 tel
christinmcmeley@dwt.com

January 5, 2018

Office of the New Hampshire Attorney General
Attn: Notification of Security Breach
33 Capitol Street
Concord, NH 03301

RECEIVED
JAN 09 2018
CONSUMER PROTECTION

Re: Report of Data Breach

To the Office of the New Hampshire Attorney General:

I represent Appen Butler Hill, Inc. ("Appen"), located at 12131 113th Ave. NE, Ste. 100, Kirkland, WA 98034-6944. Pursuant to New Hampshire Rev. Stat. § 359-C:20(I)(b), I am writing to notify you of a data security incident that may have resulted in the unauthorized access to personal information involving two (2) residents of New Hampshire. Notice of this incident was mailed to these individuals on January 5, 2018.

On October 16, 2017, Appen discovered that one of its employees had been the victim of a phishing attack. Appen immediately took measures to stop the unauthorized access, began an investigation into the matter, and has worked diligently to determine what information the attackers potentially viewed and who was potentially impacted. This included hiring a leading cybersecurity firm to support its investigation and validate its remediation efforts, as well as working to obtain log files maintained by certain of Appen's third-party service providers for the data files at issue. As a result, Appen was able to quickly ascertain an initial group of affected individuals and provided notice to those individuals and other required entities on or around November 15, 2017.

As Appen's investigation continued, it discovered that from August 11, 2017 until October 16, 2017, the attackers could have viewed certain HR files containing personal information for employees and, in some circumstances, for employees' dependents or individuals who submitted personal information associated with the employment process. Depending on the circumstances relating to each individual, the following personal information may have been accessed and acquired: full name, postal address, email address, date of birth, Social Security number, financial account information, health and disability insurance information, and copies of documents submitted with an I-9 form to establish identity and employment authorization. Appen has arranged to have ID Experts provide credit monitoring and identity repair services for three years at no cost to the affected individuals.

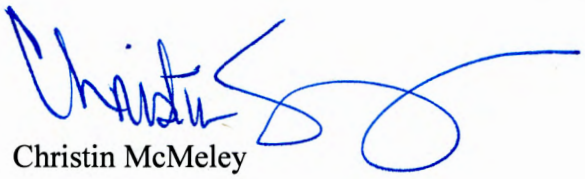
Appen is in the process of implementing additional measures with regard to security and user education designed to prevent a recurrence of a fraudulent phishing scheme.

Should a perpetrator be identified and convicted, Appen requests the opportunity to submit a victim impact statement and a request for restitution for all costs related to the breach.

Please contact me should you have any questions.

Sincerely,

Davis Wright Tremaine LLP



Christin McMeley

Enclosure: Representative sample notification letter to New Hampshire residents.

C/O ID Experts
PO Box 10444
Dublin, OH 43017-4044

To Enroll, Please Call:
(877) 982-1596
Or Visit:
www.IDExpertscorp.com/protect
Enrollment Code: [XXXXXXXX]

January 05, 2018

[FIRST NAME, LAST NAME]
[ADDRESS]
[CITY, STATE ZIP CODE]

Notice of Data Breach

Dear [FIRST NAME, LAST NAME]:

We are writing to inform you of a recent data security incident that may have resulted in unauthorized access to your personal information. We take our obligations to protect and ensure the proper use of your information very seriously. That is why, while we have no evidence that your personal information was actually compromised, we are being extremely cautious and offering you three years of identity protection services and informing you of steps we have taken and the steps you may wish to take to further protect your information. This letter supplements information you may have previously received and more fully describes what happened and what you should do now.

What Happened?

On October 16, 2017, we learned that one of our employees had been the victim of a phishing attack. Since learning of this incident, we have been diligently investigating what information the attackers potentially viewed, and who was potentially impacted. Due to the type of files potentially exposed and the fact that the files were on a third-party hosted email system, we have had our team working to obtain appropriate third party log files and collect the information necessary to notify individuals. We apologize that we were not able to complete the process sooner.

Through our investigation, we have determined that the attackers could have viewed HR files containing personal information from August 11, 2017 until October 16, 2017. In some cases, these files may have included limited personal information about dependents identified by certain Appen employees hired in 2017, or personal information submitted in 2017 by certain individuals for Appen to run a required background check. While we do not have evidence that the attackers actually viewed and acquired your personal information, despite our best efforts, we are not able to rule out the possibility.

What Information Was Involved?

It is possible that personal information may have been accessed and acquired during this exposure. In some cases, this could include full name, postal address, email address, date of birth, Social Security number, financial account information, insurance information, background check information (if a background check was necessary for your position) and copies of documents submitted with an I-9 form to establish identity and employment authorization.

What Are We Doing?

We are working with a leading cybersecurity firm to support our investigation and have taken measures to ensure the unauthorized access to our systems has been stopped. Additionally, we are in the process of implementing additional measures with regard to security and user education designed to prevent a recurrence of a fraudulent phishing scheme.

As an added precaution, we are offering you the MyIDCare identity theft protection services through ID Experts®, at no cost to you. ID Experts' fully managed recovery services will include: 36 months of Single Bureau Credit Monitoring, a $1,000,000 insurance reimbursement policy, exclusive educational materials and complete access to their fraud resolution representatives. With this protection, ID Experts will work on your behalf to resolve issues, in the event your identity is compromised.

What You Can Do:

We encourage you to enroll in the ID Experts® service at www.idexpertscorp.com/protect and use the redemption code provided above. You may enroll by phone if you prefer by calling (877) 982-1596, Monday through Friday from 8 am - 8 pm Eastern Time.

You will find detailed instructions for enrollment on the enclosed "Steps You Can Take To Further Protect Your Information" document. Also, you will need to reference your access code when calling or enrolling on the website, so please do not discard this letter.

We deeply regret any inconvenience this may cause you.

Sincerely,

Mark Brayan
CEO

Steps You Can Take To Further Protect Your Information

Minors, under the age of 18, should not have a credit history established and are under the age to secure credit. Therefore credit monitoring may not be applicable at this time. All other services provided in the membership will apply. No one is allowed to place a fraud alert on your credit report except you, please follow the instructions below to place the alert.

Website and Enrollment. Go to www.idexpertscorp.com/protect and follow the instructions for enrollment using your Access Code provided above. Once you have completed your enrollment, you will receive a welcome letter by email (or by mail if you do not provide an email address when you sign up). The welcome letter will direct you to the exclusive ID Experts' Member Website where you will find other valuable educational information.

Activate the credit monitoring provided as part of your membership with ID Experts, paid for by Appen. Credit monitoring is included in the membership, but you must personally activate it for it to be effective. **Note:** You must have established credit and access to a computer and the internet to use this service. If you need assistance, ID Experts will be able to assist you.

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity. As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

File Your Tax Return Early. Consider filing your tax returns as early as possible to minimize the chances of tax-related identity theft. If you believe you are an actual or potential victim of identity theft and would like the IRS to mark your account to identify any questionable activity, please complete *Form 14039, Identify Theft Affidavit*, available at https://www.irs.gov/pub/irs-pdf/f14039.pdf, and submit it to the appropriate address per the form instructions. Additional information on ways you can reduce your risk and steps you can take if you believe you have become a victim of tax-related identity theft can be found in the IRS's *Taxpayer Guide to Identity Theft*, available at https://www.irs.gov/newsroom/taxpayer-guide-to-identity-theft.

Obtain a Copy of Your Credit Report. You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

TransUnion	**Experian**	**Equifax**	**Free Annual Report**
P.O. Box 1000	P.O. Box 9532	P.O. Box 105851	P.O. Box 105281
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-877-322-8228	1-888-397-3742	1-800-525-6285	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	annualcreditreport.com

Place a Fraud Alert on Your Credit Report. You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Place a Security Freeze on Your Credit File. In some US states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. If you request a security

freeze from a consumer reporting agency there may be a fee up to $10 to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources on Identity Theft: You can obtain information from the consumer reporting agencies, Federal Trade Commission or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the Federal Trade Commission or to the Attorney General in your state. Residents of North Carolina can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
ftc.gov/idtheft
1-877-438-4338

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

2018 JAN -9 AM 10: 08
DEPT OF JUSTICE
STATE OF NH