LEWIS BRISBOIS BISGAARD & SMITH LLP

Sean B. Hoar
888 SW Fifth Avenue, Suite 900
Portland, Oregon 97204-2025
Sean.Hoar@lewisbrisbois.com
Direct: 971.712.2795

April 14, 2021

VIA E-MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
Department of Justice
33 Capitol Street
Concord, NH 03301
E-Mail: doj.cpb@doj.nh.gov

Re: Notification of Data Security Incident

Dear Attorney General MacDonald:

We represent APC Workforce Solutions, LLC ("APC") and its subsidiaries Quick Search, Employment Screening Solutions ("ESS"), and Quick Courtlinks, located in Orlando, Florida. This letter is being sent because APC determined that personal information of New Hampshire residents may have been affected by a data security incident. The incident may have involved unauthorized access to the New Hampshire residents' Social Security numbers, names, and addresses.

On December 21, 2020, APC detected a data security incident that disrupted access to systems in its IT environment. It immediately took steps to contain the incident and secure its environment, and launched an investigation with the support of outside data security experts. On February 23, 2020, the investigation determined that the personal information of 30 New Hampshire residents may have been affected.

APC notified the New Hampshire residents with the attached letter on April 7, 2021 and the individuals were offered 12 months of complimentary credit monitoring and identity restoration services through Kroll, a global leader in risk mitigation and response. A sample copy of the notification letter to the affected individuals is included with this correspondence. Should you have any questions or need additional information, please contact me at (971) 712-2795 or via email at Sean.Hoar@lewisbrisbois.com.

Sincerely,

/s/ Sean B. Hoar

Sean B. Hoar of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl.: Sample Consumer Notification Letter

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Notice of Data Security Incident

Dear <<first_name>>,

I am writing to inform you of a data security incident involving individuals who utilized employment screening services provided by Quick Search, Employment Screening Solutions ("ESS"), and Quick Courtlinks.[1] We take the privacy and security of your information very seriously. This is why we are writing to inform you of the incident and steps you can take to help protect your personal information.

What Happened. On December 21, 2020, the operations team supporting these employment screening services detected a data security incident that temporarily disrupted access to a small subset of IT systems. They immediately took steps to secure the environment and minimize the impact from the incident. An investigation into the incident was immediately launched with the support of multiple outside data security experts. The investigation determined that while the issue was limited to a small portion of IT systems, some personal information was accessed without authorization.

What Information Was Involved. The information involved your <<b2b_text_1(ImpactedData)>>.

Please note that receiving this letter does not mean you are a victim of identity theft. Instead, this letter is provided and identity monitoring is being offered out of an abundance of caution, and for the ongoing security of your information.

What We Are Doing. As soon as we discovered the incident, we took the steps described above. Upon detecting the incident, we immediately took action to prevent any further unauthorized activity. Our IT professionals enhanced system security to help prevent a similar incident from occurring in the future. Among other things, this included resetting administrative and user passwords and deploying advanced security tools. We also contacted law enforcement and will provide whatever cooperation is necessary to hold the perpetrators accountable.

We have also secured the services of Kroll to offer you 12 months of identity monitoring services at no cost to you. Kroll is a global leader in risk mitigation and response. Below you will find information on signing up for the complimentary 12-month membership, as well as steps you can take to help further protect your online information.

What You Can Do. We recommend that you review the guidance included with this letter about how to help protect your online information. You can also activate the complimentary 12 months of Kroll identity monitoring services, including Credit Monitoring, Web Watcher, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

You have until ***June 24, 2021*** to activate your identity monitoring services.

Membership Number: **<<Member ID>>**

Additional information describing your services is included with this letter.

[1] Quick Search, ESS and Quick Courtlinks are subsidiaries or divisions of APC Workforce Solutions, LLC, 420 S. Orange Avenue, Orlando, FL 32801, Attn: General Counsel.

If you have questions or need assistance, please contact (855) 688-0531. Kroll representatives are available to assist you Monday through Friday from 9:00 a.m. - 6:30 p.m. Eastern Time.

For More Information. Further information about how to help protect your online personal information appears on the following page. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Katrina Adams

Katrina Adams
Director, Employment Screening
Quick Search, Quick Courtlinks, and ESS

Steps You Can take to Help Protect Your Personal Information

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).

Copy of 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 1-877-322-8228, 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 also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: 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 one year. 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.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. 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. 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: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

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

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

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

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.