BakerHostetler

Baker&Hostetler LLP

1170 Peachtree Street
Suite 2400
Atlanta, GA 30309-7676

T 404.459.0050
F 404.459.5734
www.bakerlaw.com

John P. Hutchins
direct dial: 404.946.9812
jhutchins@bakerlaw.com

November 30, 2021

VIA E-MAIL (CONSUMER@AG.IOWA.GOV)

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

Re: Incident Notification

Dear Sir or Madam:

We are writing on behalf of our client Bansley and Kiener, L.L.P. ("Bansley"), to notify your office of a cyber security incident.

Bansley completed an investigation into a security incident involving potential unauthorized access to data maintained on its systems. Upon learning of the incident, Bansley secured its systems. It investigated the incident and a cybersecurity firm was engaged to assist. The investigation determined that an unauthorized person gained access to Bansley's systems between August 20, 2020 and December 1, 2020. The names and Social Security numbers of 2,518 Iowa residents were involved.

On November 30, 2021, Bansley will begin mailing notification letters to 2,518 Iowa residents in accordance with Iowa Code § 715C.1-2, via United States First-Class mail. A copy of the notification letter is enclosed. Bansley is offering the Iowa residents access to complimentary one-year subscriptions to credit monitoring, fraud consultation, and identity restoration services through Kroll. This service helps detect possible misuse of personal information and provides identity theft protection services focused on immediate identification and resolution of identity theft. A dedicated, toll-free call center has been established for individuals to call with questions regarding the incident.

To help prevent a similar incident from occurring in the future, Bansley has taken steps to confirm and further strengthen the security of its systems, including deploying watchguard,

firewall upgrades, establishing and reviewing permissions for secure portals and Sharefile systems, resetting user passwords, and transferring sensitive data to cloud storage. Bansley also continues to educate its employees on cyber security best practices.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

John P. Hutchins

John P. Hutchins
Partner

Enclosure

BANSLEY AND KIENER, L.L.P.
CERTIFIED PUBLIC ACCOUNTANTS

<<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 BREACH

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Bansley and Kiener, L.L.P. is a full service accounting firm that has conducted payroll compliance engagements for health, pension, and other benefit plans in the Midwest region, in which you may have been a participant. We are writing to notify you of a security incident that may have involved some of your personal information. This notice explains the incident, what information was involved, steps taken since discovering the incident, and some steps you may consider taking in response.

What Happened?

On December 10, 2020, we identified a data security incident that resulted in the encryption of certain systems within our environment. We addressed the incident, made upgrades to certain aspects of our computer security, restored the impacted systems from recent backups, and resumed normal operation. We believed at the time that the incident was fully contained and did not find any evidence that information had been exfiltrated from our environment.

On May 24, 2021, we were made aware that certain information had been exfiltrated from our environment by an unauthorized person. We immediately launched an investigation, and a cyber security firm was engaged to assist.

What Information Was Involved?

We cannot confirm specifically what information, if any, was viewed by the unauthorized person. However, on August 24, 2021, the investigation confirmed that the information present on our systems at the time of the incident (i.e., information that was accessed by the unauthorized person) included your full name and Social Security number.

What We Are Doing?

Information privacy and security are among our highest priorities. We have strict security measures in place to protect information in our care. Upon learning of the incident, and to help prevent something like this from happening in the future, we have taken steps to confirm and further strengthen the security of our systems, including deploying SentinelOne Endpoint Detection & Response software on the computers in our environment, upgrading our filtering capabilities to block traffic from malicious sources, establishing and reviewing permissions for secure file share portals, resetting user passwords, and transferring sensitive data to cloud storage. We also continue to educate our employees on cyber security best practices.

We are notifying individuals whose information was involved, including you, so that you may take further steps to protect your personal information should you feel it is appropriate to do so.

What Can You Do?

As a precautionary measure, we also secured the services of Kroll to provide identity monitoring services at no cost to you for one (1) year. Your identity monitoring services include credit monitoring, fraud consultation, and identity theft restoration.

These services are completely free to you and activating these services will not hurt your credit score.

For more information about Kroll's identity monitoring, including instructions on how to activate your complimentary one-year membership, please visit the below website:

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

You have until <<b2b_text_6 (Activation Deadline)>> to activate your identity monitoring services.

Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Further, it is always advisable for you to regularly review your financial account statements and credit reports for unauthorized activity. If you notice such activity, you should immediately report it to the relevant financial institution or the credit bureau reporting the activity. You may also review the information contained in the enclosed "Additional Steps You Can Take."

For More Information.

We understand you may have questions about the incident. To ensure your questions are answered in a timely manner, we established a dedicated assistance line at 1-855-732-0782 which can be reached Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding some U.S. holidays. A copy of this notice is also available at *www.bk-cpa.com* for reference.

We take the privacy and security of the personal information in our care very seriously. We sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

Beasley and Kiesen, L.L.P.

ATENCIÓN: si habla español, tiene a su disposición servicios gratuitos de asistencia lingüística; llame al 1-855-732-0782.

ADDITIONAL STEPS YOU CAN TAKE

To help relieve concerns and restore confidence following the incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience in helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include credit monitoring, fraud consultation, and identity theft restoration.

- Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.
- *You have until* ***<<b2b_text_6 (Activation Deadline)>>*** *to activate your identity monitoring services.*
- Membership Number: **<<Membership Number s_n>>**

Additional information describing your services is included with this letter.

If you prefer to activate these services offline and receive monitoring alerts via the US Postal Service, you may activate via our automated phone system by calling 1-888-653-0511, Monday through Friday, 8:00 a.m. to 5:30 p.m. Central time, excluding major U.S. holidays. Please have your membership number located in your letter ready when calling. Please note that to activate monitoring services, you will be required to provide your name, date of birth, and Social Security number through our automated phone system.

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Bansley and Kiener, L.L.P. can be contacted at 8745 West Higgins Road, Suite 200, Chicago, IL 60631, or by phone at (312) 263-2700.

Connecticut: You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

District of Columbia: You may contact and obtain information from your attorney general at: Office of the Attorney General for the District of Columbia, 441 4th Street NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

Massachusetts: Under Massachusetts law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Office of the Massachusetts Attorney General*, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

West Virginia: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.

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.

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.