WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

July 23, 2021

Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

Via Certified Mail; Return Receipt Requested

Attorney General Lawrence Wasden
Office of the Attorney General
State of Idaho
700 W. Jefferson Street, Suite 210
P.O. Box 83720
Boise, Idaho 83720-0010

Re: Cybersecurity Incident Involving Heaton & Company PLLC dba Pinnacle Accountancy Group of Utah

Dear Attorney General Wasden:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Heaton & Company PLLC dba Pinnacle Accountancy Group of Utah ("Pinnacle"), an accounting firm located in Farmington, Utah, with respect to a recent cybersecurity incident that was first discovered by Pinnacle on April 17, 2021 (hereinafter, the "Incident"). Pinnacle takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the Incident, what information may have been compromised, the number of Idaho residents being notified, and the steps that Pinnacle has taken in response to this incident. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring services.

1. Nature of the Incident

On April 17, 2021, Pinnacle discovered the Incident when some of the Pinnacle's client files were found to have been deleted from Pinnacle's systems by an unauthorized individual. Upon discovery of the incident, Pinnacle promptly engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the incident. While the forensic investigation did not find any evidence to support data exfiltration, there were evidence that some of the client data may have been accessed by an unauthorized individual. Pinnacle immediately began a thorough review of the potentially accessed files to identify the clients whose sensitive information was present at the time of the incident. This step was necessary so that Pinnacle could send a notice of the incident to ensure the potentially impacted clients are aware of this incident.

Although Pinnacle is unaware of any fraudulent misuse of information, it is possible that clients' name, address, date of birth, social security number, employer identification number, and financial

account number may have been exposed as a result of this unauthorized activity. However, the types of information impacted varied by clients and not all clients were affected by this incident.

As of this writing, Pinnacle has not received any reports of related identity theft since the date of the incident (April 17, 2021 to present).

2. Number of Idaho residents affected.

Pinnacle identified and notified 312 clients who were potentially affected by this Incident. Of those, one (1) was a resident of Idaho. Notification letter to this individual was mailed on July 23, 2021, by first class mail. A sample copy of the notification letter being mailed to the potentially affected Idaho resident is included with this letter under **Exhibit A**.

3. Steps taken in response to the Incident.

Pinnacle takes the security and privacy of all client information very seriously, and has taken steps to protect the privacy and security of potentially impacted individuals' information. Specifically, upon discovery of this Incident, Pinnacle immediately engaged a specialized cybersecurity firm to determine the full nature and scope of the Incident. Additionally, Pinnacle restored its systems in a safe and secure mode, and was able to recover its files from backups. Pinnacle also enhanced the security of its computer systems and servers, and implemented two-factor authentication. Lastly, Pinnacle informed our law firm and began identifying the potentially affected individuals in preparation for notice.

Although Pinnacle is not aware of any evidence of misuse of personal information, Pinnacle provided the potentially impacted individuals with complimentary services to help protect their identity. Specifically, Pinnacle has arranged for the impacted individuals to enroll in credit monitoring services (including identity theft protection) provided by Kroll at no cost to them for 12 months.

4. Contact information

Pinnacle remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Anjali C. Das

EXHIBIT A

PINNACLE
Accountancy Group of Utah
Certified Public Accountants
a dba of
Heaton & Company, PLLC

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

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

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Heaton & Company PLLC d/b/a Pinnacle Accountancy Group of Utah ("Pinnacle") is writing to notify you of a recent data security incident that may affect the privacy of some of your personal information. While we are unaware of any fraudulent misuse of your personal information at this time, we are providing you with information about the incident, steps we have taken in response, and resources available to help you protect against the possible misuse of your information.

What Happened?

On April 17, 2021, Pinnacle discovered the data security incident when some of the Pinnacle's client files were found to have been deleted from Pinnacle's systems by an unauthorized individual. Upon discovery of the incident, Pinnacle promptly engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the incident. While the forensic investigation did not find any evidence to support data exfiltration, there were evidence that some of the client data may have been accessed by an unauthorized individual. Pinnacle immediately began a thorough review of the potentially accessed files to identify the clients whose sensitive information was present at the time of the incident. This step was necessary so that Pinnacle could send this notice of the incident to ensure that you are aware of this incident.

What Information Was Involved?

The types of information impacted varied by individual. However, the information present in the folders may have included your name, address, date of birth, Social Security number, employer identification number, and/or financial account number.

What We Are Doing

We are committed to doing everything we can to help protect the privacy and security of the personal information in our care. Since the discovery of the incident, we have taken and will continue to take steps to mitigate the risk of future issues. Notably, we were able to recover our files from backups and restored our systems in a safe and secure mode. We also enhanced the security of our computer systems and servers, and implemented two-factor authentication. We are also providing you with guidance on how to help protect against the possibility of information misuse.

Out of an abundance of caution, we are also providing you with 12 months of complimentary identity monitoring services through Kroll. While we are covering the cost of these services, you will need to complete the activation process by following the instructions included in the enclosed *Steps You Can Take to Help Protect Your Information.*

What You Can Do

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

You may also activate the identity monitoring services we are making available to you. Again, we are making these services available to you at no cost; however, you will need to activate yourself in these services. The deadline to activate is October 24, 2021.

We would like to reiterate that, at this time, there is no evidence that your information was misused. However, we encourage you to take full advantage of the services offered.

For More Information

We recognize that you may have questions not addressed in this letter. If you have additional questions, please call 1-XXX-XXX-XXXX (toll free) during the hours of 8:00 a.m. and 5:30 p.m. Central Time, Monday through Friday (excluding U.S. national holidays).

Pinnacle sincerely regrets any inconvenience or concern that this matter may cause, and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

Cameron J. Pribble, CPA
Heaton & Company PLLC d/b/a Pinnacle Accountancy Group of Utah

Steps You Can Take to Help Protect Your Information

To help relieve concerns and restore confidence following this 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 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 October 24, 2021 to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

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.

Additional Important Information

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone or online. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-525-6285
www.experian.com/fraud/center.html	www.transunion.com/fraud-alerts	https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Experian	TransUnion	Equifax
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-888-298-0045
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	https://www.equifax.com/personal/credit-report-services/credit-freeze/

More information can also be obtained by contacting the Federal Trade Commission:

Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov.

For residents of *Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia, and Wyoming*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Colorado, Illinois, Iowa, Maryland, Missouri, New Mexico, North Carolina, Oregon,* and *West Virginia*: It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *New Mexico*: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach.

For residents of *Massachusetts*: It is required by state law that you are informed of your right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For residents of *Oregon*: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of *Rhode Island*: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

For residents of Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina, and Rhode Island: You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

District of Columbia Office of the Attorney General – Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Illinois office of the Attorney General - 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - Consumer Protection Division: 200 St. Paul Place, 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

New York Office of Attorney General - Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; https://ag.ny.gov/consumer-frauds/identity-theft

North Carolina Office of the Attorney General - Consumer Protection Division: 9001 Mail Service Center, Raleigh, NC 27699; 1-877-566-7226; www.ncdoj.com

Rhode Island Office of the Attorney General - Consumer Protection: 150 South Main St., Providence RI 02903; 1-401-274-4400; www.riag.ri.gov