CONSTANGY
BROOKS, SMITH & PROPHETE LLP

September 14, 2023

VIA EMAIL: DOJ-CPB@doj.nh.gov

Attorney General John Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
Phone: (603) 271-3643
Fax: (603) 271-2110

Re: Notification of Data Security Incident

Dear Attorney General Formella:

Constangy, Brooks, Smith & Prophete, LLP represents Birch Horton Bittner & Cherot ("BHBC"), a law firm with offices in Anchorage, Alaska, and Washington, D.C., in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with New Hampshire's data breach notification statute, N.H. Rev. Stat. §§ 359-C:19 - C:21.

1. **Nature of the Security Incident**

On or about July 26, 2023, BHBC discovered that an unauthorized party was able to gain access to part of its network environment. In response, BHBC immediately began an internal investigation and secured its network. BHBC also engaged third-party cybersecurity experts to determine what happened, including whether any personal information was impacted. That investigation continues. However, on or about August 4, 2023, BHBC confirmed that personal information of its employees was acquired by an unauthorized threat actor in conjunction with this incident.

BHBC is notifying all current employees of the incident, providing them with steps they can take to protect their personal information, and offering them the opportunity to enroll in credit and identity monitoring services at no cost to them.

2. **Number of Affected New Hampshire Residents & Information Involved**

The incident involved personal information for approximately 1 New Hampshire resident. The information involved in the incident may differ depending on the individual but may include the following for affected New Hampshire residents: Name in combination with a ,

.

3. **Notification to Affected Individuals**

On September 7, 2023, a notification letter was sent to the affected New Hampshire resident by USPS First Class Mail and via electronic mail. The notification letter provides resources and steps individuals can take to help protect their information. The notification letter also offers each individual the opportunity to enroll in of complimentary identity protection services, including Three Bureau Credit Monitoring/Three Bureau Credit Report/Three Bureau Credit Score services, dark web monitoring, $1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. Those services are offered by Cyberscout through Identity Force, a TransUnion company. This service includes consumer access to a call center for 90 days to answer questions and assist with enrollment. A sample notification letter is enclosed.

4. **Measures Taken to Address the Incident**

In response to the incident, BHBC retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise. BHBC has implemented additional security measures to further harden its network environment in an effort to prevent a similar event from occurring in the future.

Finally, BHBC is notifying affected employees and providing them with steps they can take to protect their personal information as discussed above. As the investigation continues, additional notifications may be forthcoming.

5. **Contact Information**

If you have any questions or need additional information regarding this incident, please do not hesitate to contact me at .

Sincerely,

Donna Maddux of
Constangy, Brooks, Smith & Prophete LLP

Birch Horton Bittner & Cherot
a professional corporation

September 7, 2023

VIA U.S. MAIL &
ELECTRONIC DELIVERY
[redacted]

[redacted]

Re: Notice of Data Security Incident

Dear [redacted],

Birch Horton Bittner & Cherot ("BHBC") takes the privacy and security of your information extremely seriously. We are writing to formally inform you of a recent data security incident that involved your personal information. Please read this letter carefully as it contains information regarding the incident and steps you can take to help protect your personal information, including the opportunity to enroll in twenty-four (24) months of complimentary credit monitoring and identity protection services.

What happened? On or about July 26, 2023, BHBC discovered that an unauthorized party was able to gain access to part our network environment through a third-party vendor who had access to our system. In response, we immediately began an internal investigation and secured our network. We also engaged third-party cybersecurity experts to determine what happened, including whether any personal information was impacted. That investigation continues. However, on or about August 4, 2023 we confirmed that personal information of our employees was acquired by an unauthorized threat actor in conjunction with this incident.

What Information Was Involved? Based upon our initial investigation, it appears that the data taken for each employee varies, but may include your

What We Are Doing. In addition to the steps described above, we implemented additional security measures to further protect our network environment and minimize the likelihood of future incidents. We are also providing you with access to Three Bureau Credit Monitoring/Three Bureau

Credit Report/Three Bureau Credit Score services, at no charge to you. These services provide you with credit alerts for 24 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do. We recommend that you review the guidance included with this letter about how to protect your information. To enroll in Credit Monitoring services at no charge, please log on to and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

The privacy and security of your information is a top priority for Birch Horton Bittner & Cherot. We take this incident very seriously and we regret any worry or inconvenience this may cause you.

Sincerely,

BIRCH HORTON BITTNER & CHEROT

Aaron D. Sperbeck
Partner
510 L Street, Suite 700
Anchorage AK 99501

ADDITIONAL STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR 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 monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. 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). 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 Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft.

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 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:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 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 Alerts: There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts 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. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary poof. An extended fraud alert is also free and will stay on your credit report for seven years. 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. Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze 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. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the Federal Trade Commission identified above. 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. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the 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 via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after receiving your request.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right 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. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

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.

Additional information:

District of Columbia: The Office of the Attorney General for the District of Columbia can be reached at 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov

Maryland: Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 888-743-0023; oag@state.md.us or IDTheft@oag.state.md.us