



Jason Cherry, Partner
Cybersecurity & Data Privacy Team
2029 Century Park East
Los Angeles, CA 90067
Telephone: 207.745.1397

November 12, 2024

VIA U.S. MAIL

Attorney General Anthony G. Brown
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Notice of Data Security Incident

To Whom it May Concern:

Constangy, Brooks, Smith & Prophete, LLP (“Constangy”) represents Butt Thornton and Baehr PC (“BTB”), a law firm in New Mexico, in connection with a data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maryland’s data breach notification statute.

1. Nature of the Security Incident

On June 5, 2024, BTB discovered unusual activity associated with an employee’s email account. BTB immediately took steps to secure its email environment and engaged cybersecurity experts to conduct an investigation to determine what happened. The investigation conducted by the third-party cybersecurity experts determined that an unknown actor may have acquired certain data without authorization. BTB then worked with additional experts to conduct a comprehensive review of the affected data to determine whether personal information may have been affected. This process was completed on October 28, 2024.

2. Number of Affected Maryland Residents & Information Involved

On November 12, 2024, BTB notified three (3) Maryland residents.

The information involved in the incident for the affected Maryland residents may have included name and Social Security number.

3. Notification of Affected Individuals

On November 12, 2024, a notification letter was mailed to the affected Maryland residents by USPS First Class Mail. The notification letter provides resources and steps the individuals can take to help protect their information. The notification letter also offers the opportunity to enroll in twelve (12) months of complimentary identity protection services, including credit monitoring,

November 12, 2024

Page 2

identity protection services and a call center, should the individuals have questions about the incident. Those services are offered by TransUnion, a company specializing in fraud assistance and remediation services. A sample notification letter sent to the impacted individuals is included with this correspondence.

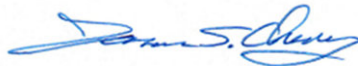
4. Steps Taken to Address the Incident

In response to the incident, BTB retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise. BTB also implemented additional security measures to further harden its digital environment in an effort to prevent a similar event from occurring in the future. Finally, BTB is notifying the affected individuals and providing them with steps they can take to protect their personal information as discussed above.

5. Contact Information

BTB remains dedicated to protecting the information in its control. If you have any questions or need additional information, please do not hesitate to contact me at jcherry@constangy.com or 207.745.1397.

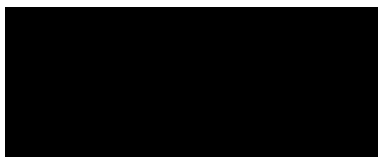
Sincerely,

A handwritten signature in blue ink, appearing to read "Jason S. Cherry".

Jason Cherry of
CONSTANGY, BROOKS, SMITH & PROPHETE LLP

Enclosure: Consumer Notification Letter

Butt Thornton & Baehr PC
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



November 12, 2024

Subject: Notice of Data Security Incident

Dear [REDACTED]:

Butt Thornton & Baehr PC ("BTB") is writing to inform you of a recent data security incident that may have affected your personal information. We take the privacy and security of all personal information within our possession very seriously. This letter contains information regarding the incident and steps you can take to help protect your personal information.

What Happened. On June 5, 2024, we discovered unusual activity associated with an employee's email account. We immediately engaged experts to help us secure the environment and investigate what happened. The investigation determined that an unknown actor acquired certain data without authorization. We then conducted a comprehensive review of the affected account to determine whether personal information may have been involved. After a thorough review of the data, on October 28, 2024, it was determined that some of your personal information was present. We then took steps to notify you of the incident as quickly as possible.

What Information Was Involved. The information involved may have included your name and [REDACTED].

What We Are Doing. As soon as we discovered the incident, we took the steps described above and attempted to minimize the risk of a similar incident occurring in the future.

We are also offering you access to credit monitoring services at no charge. These services provide you with alerts for twelve 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 victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log onto <https://bfs.cyberscout.com/activate> 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. 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.

000010102G0500

P

What You Can Do. You can follow the recommendations on the following page to help protect your personal information. We also encourage you to enroll in the complimentary services being offered to you through Cyberscout by using the enrollment code provided.

For More Information: Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call Cyberscout at 1-800-405-6108 from 8:00 AM to 8:00 PM Eastern Time, Monday through Friday (excluding holidays).

We take this event and the security of information in our care seriously. We regret any concern or inconvenience that this incident may cause you.

Sincerely,

Butt Thornton & Baehr PC
4101 Indian School Road NE
Ste 300
Albuquerque, NM 87110

STEPS YOU CAN TAKE TO HELP 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 proof. 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 <https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.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; <https://oag.dc.gov/>

California: The California Attorney General can be reached at: 1300 "I" Street, Sacramento, CA 95814-2919; 800-952-5225; <http://oag.ca.gov/>

Maryland: The 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; <https://www.marylandattorneygeneral.gov/>

North Carolina: The North Carolina Attorney General's Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; <https://ncdoj.gov/>

New York: The New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005; 212-416-8433; <https://ag.ny.gov/>

Rhode Island: The total number of individuals receiving notification of this incident is 2. The Rhode Island Attorney General can be reached at: 150 South Main Street Providence, RI 02903, <http://www.riag.ri.gov>

Texas: The Texas Attorney General can be reached at: 300 W. 15th Street, Austin, Texas 78701; 800-621-0508; texasattorneygeneral.gov/consumer-protection/

Vermont: The Vermont Attorney General's Office can be reached at: 109 State Street, Montpelier, VT 05609; 802-828-3171; ago.info@vermont.gov; <https://ago.vermont.gov/>