



Alyssa Watzman, Partner
Cybersecurity & Data Privacy Team
1801 Broadway, Suite 520
Denver, CO 80202
AWatzman@constangy.com
Direct: 720.536.3234

November 6, 2024

VIA EMAIL

Attorney General Anthony G. Brown
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Email: Idtheft@oag.state.md.us

Re: Notification of Data Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith, and Prophete LLP represents Kevin Leeds, CPA, PC (“Kevin Leeds, CPA”) – a tax, accounting, and consulting firm – 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 compliance with Maryland’s data breach notification statute.

1. Nature of the Security Incident

On January 29, 2024, Kevin Leeds, CPA became aware of unusual activity that disrupted access to certain computer systems. Upon discovering this activity, Kevin Leeds, CPA took immediate steps to secure its digital environment and engaged independent cybersecurity experts to assist with an investigation. As a result, Kevin Leeds, CPA learned that an unknown actor gained access to certain data on its network. On or about October 14, 2024, Kevin Leeds, CPA learned that personal information was impacted in connection with this incident and worked to provide notification to potentially impacted individuals as quickly as possible.

2. Number of Affected Maryland Residents Notified

On November 6, 2024, Kevin Leeds, CPA notified eleven (11) Maryland residents by letter mailed via first class U.S. mail. A sample copy of the notification letter is included with this correspondence.

The impacted information varied by individual, but may have included the residents’ Social Security number.

3. Measures Taken to Address the Incident

Upon discovering the incident, Kevin Leeds, CPA took the steps referenced above. Kevin Leeds, CPA also implemented additional security measures to further harden its environment in an effort to prevent a similar event from occurring in the future. Kevin Leeds, CPA also reported this incident to federal law enforcement and will cooperate with any investigation.

Kevin Leeds, CPA is also notifying the affected individuals and providing resources and steps individuals can take to help protect their information. The notification letter offers each individual complimentary credit monitoring and identity protection services through IDX by Zerofox. These services include 12 months of credit and CyberScan dark web monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. IDX will also support a call center to answer questions and assist with enrollment.

4. Contact Information

Kevin Leeds, CPA takes the privacy and security of all information in its possession very seriously. If you have any questions or need additional information, please do not hesitate to contact me at AWatzman@constangy.com and David Rice at DRice@constangy.com.

Best Regards,

/s/ Alyssa Watzman

Alyssa Watzman
CONSTANGY, BROOKS, SMITH &
PROPHETE LLP

Encl.: Sample Notification Letter



P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

November 6, 2024

Subject: Notice of Data <<Variable Text 1: Breach or Security Incident>>

Dear << First Name>> << Last Name>>:

The purpose of this communication is to notify you of a data security incident experienced by Kevin Leeds, CPA, PC ("Kevin Leeds, CPA") which affected your personal information. Please read this letter carefully as it contains details about the incident and resources you can utilize to protect your information, including instructions for enrolling in complimentary credit monitoring and identity theft protection services.

What Happened? On January 29, 2024, Kevin Leeds, CPA became aware of unusual activity that disrupted access to certain computer systems. Upon discovering this activity, we took immediate steps to secure our digital environment. We also engaged leading, independent cybersecurity experts to assist with an investigation and to determine whether personal information was impacted. The investigation revealed that an unknown actor was able to access certain data from our network. On or about October 14, 2024, we learned that your personal information was impacted in connection with this incident.

What Information Was Involved? The information involved included your name along with your <<Variable Text 2: Potentially Impacted Data Sets>>.

What We Are Doing. As soon as Kevin Leeds, CPA discovered this incident, we took the steps referenced above. We also implemented additional security features to reduce the risk of a similar incident occurring in the future. In addition, we notified the Federal Bureau of Investigation and will provide whatever cooperation is necessary to hold the perpetrators of this incident accountable, if possible.

Kevin Leeds, CPA is also providing you with the opportunity to enroll in complimentary credit monitoring and identity theft protection services through IDX – a data breach and recovery services expert. These services include: <<12/24 months>> of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. To receive credit monitoring 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. Please note that the deadline to enroll is February 6, 2025.

What You Can Do. We encourage you to enroll in the credit monitoring and identity protection services we are offering, which are at no cost to you. Please also review the guidance included with this letter which includes additional resources you may use to help protect your information.

For More Information. Representatives at IDX are available to assist you with enrolling in the services being offered and answer questions you may have regarding this incident, between the hours of 9:00 a.m. to 9:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the call center toll-free at (833) 903-3648 and provide the representative with your unique code listed above.

On behalf of Kevin Leeds, CPA, we thank you for your understanding about this incident. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Very truly yours,

Kevin Leeds, CPA, PC
207 Spring Valley Ave
Maywood, NJ 07607

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 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 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

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

Maine: Maine Attorney General can be reached at: 6 State House Station Augusta, ME 04333; 207-626-8800; <https://www.maine.gov/ag/>

Maryland: Maryland Attorney General can be reached at: 200 St. Paul Place, Baltimore, MD 21202; 888-743-0023; <https://www.marylandattorneygeneral.gov/>

Minnesota: Minnesota Attorney General can be reached at: 445 Minnesota Street, Suite 1400, St. Paul, MN 55101; 651-296-3353; <https://www.ag.state.mn.us/>

North Carolina: 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; www.ncdoj.gov

New York: 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: Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, RI 02903; 401-274-4400; <http://www.riag.ri.gov>

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

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