



James M. Paulino, Esq.
Innovation Square
100 South Clinton Ave, Ste. 1620
Rochester, New York 14604
jpaulino@constangy.com
Tel: 585.281.3000

April 16, 2024

VIA ONLINE SUBMISSION

Attorney General Aaron Frey
Office of the Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall Street, 6th Floor
Augusta, ME 04330

Dear Attorney General Frey:

Constangy, Brooks, Smith and Prophete LLP (“Constangy”) represents HBL CPAs, P.C. (“HBL”) in connection with an incident described in greater detail below. The purpose of this letter is to notify you, in accordance with Maine statute, that this incident may have affected the personal information of 2 Maine residents. HBL hereby reserves all rights and defenses in connection herewith.

1. Nature of Incident

On November 30, 2023, HBL became aware of unusual activity in its network environment. HBL immediately took steps to secure its digital environment and conducted an investigation to assess the full nature and scope of the event. The investigation revealed that an unknown actor gained access to HBL systems and may have accessed or obtained certain data on or around November 30, 2023. HBL then worked with additional experts to conduct a comprehensive review of the impacted data to determine what personal information was involved. On or about April 5, 2024, HBL identified individuals whose personal information may have been contained within potentially impacted files, and HBL has taken steps to prepare and send letters to potentially impacted individuals along with an offer of complimentary credit and identity monitoring services.

The potentially impacted information may have included individuals’ names along with their Social Security Numbers, driver license numbers, and tax Identity Protection PINs.

2. Number of Maine residents affected

HBL notified 2 Maine residents of the incident via first class U.S. mail on April 16, 2024. A sample copy of the notification letter is included with this correspondence.

3. Steps taken relating to the incident

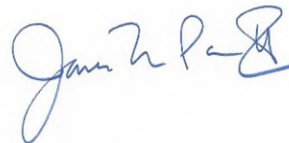
Upon discovering the issue, HBL took the steps described above. HBL notified the Federal Bureau of Investigation (“FBI”) and the Internal Revenue Service (“IRS”), and will provide whatever cooperation is necessary to hold the perpetrators accountable, if possible. HBL has also worked

with the IRS and the IRS Stakeholder Liaison to take protections against fraudulent tax filings, and provided notice of the incident to potentially impacted individuals on April 16, 2024. In addition, HBL is offering affected individuals 12 months of credit monitoring, identity restoration services, and identity protection insurance through Cyberscout Identity Force, a TransUnion company. HBL has also provided guidance on steps individuals can take to protect personal information.

4. Contact information

If you have any questions or need additional information, please do not hesitate to contact me at 585.281.3000 or jpaulino@constangy.com.

Very truly yours,

A handwritten signature in blue ink, appearing to read "James M. Paulino, Esq.", with a stylized flourish at the end.

James M. Paulino, Esq. of
Constangy, Brooks, Smith & Prophete, LLP

Encl.: Sample Consumer Notification Letter

HBL CPAs, P.C.
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
«uniqueid» «ctn_no»-«pkg_no_ctn»



«firstname» «lastname»
«address1» «address2»
«city», «state» «postalcode4»-«zip4»
«imb_encode»

April 16, 2024

«custom_field_1»

Dear «firstname» «lastname»:

HBL CPAs, P.C. (“HBL”) is writing to inform you of a recent incident that may have involved your personal information. Please review the following for more information about the incident, steps you can take to help protect your personal information, and an offer of complimentary credit monitoring and identity protection services.

What Happened? On November 30, 2023, HBL became aware of unusual activity in our network environment. We immediately took steps to secure our digital environment and conducted an investigation to assess the full nature and scope of the event. The investigation revealed that an unknown actor gained access to HBL systems and may have accessed or obtained certain data on or around November 30, 2023. HBL then worked with additional experts to conduct a comprehensive review of the impacted data to determine what personal information was involved. On or about April 5, 2024, we determined that your personal information may have been impacted in connection with this incident.

What Information Was Involved? The information involved included your name along with your «exposed_data_elements».

What We Are Doing? As soon as we 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. We notified the Federal Bureau of Investigation and will provide whatever cooperation is necessary to hold the perpetrators accountable, if possible.

We also promptly notified the Internal Revenue Service and have been working with the IRS Stakeholder Liaison to protect against fraudulent filings, including enrolling all clients in the eFiling “opt-in” program requiring specific coordination with the IRS prior to filing. We are encouraging you to consider requesting an IRS PIN, as an additional six-digit code to authenticate your identity when you file your electronic or paper tax return. If you do not already have an IRS PIN, you may get one as a proactive step to protect yourself from tax-related identity theft either online, by paper application or in-person. Information about the IRS PIN program can be found here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

HBL is also notifying you of this incident and offering you the opportunity to enroll in Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for «service_length» 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.

To enroll, please go to <https://bfs.cyberscout.com> and use the Enrollment Code «**uniquecode**». Cyberscout representatives are available for 90 days from the date of this letter to assist you with questions regarding enrollment between 6:00 am – 6:00 pm Mountain Time, Monday through Friday, excluding holidays. Please note the deadline to enroll is July 15, 2024. 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.

What You Can Do. We encourage you to enroll in the complimentary identity protection services we are offering. Please also review the guidance at the end of this letter which includes additional resources you may utilize to help protect your information.

For More Information: Cyberscout Representatives are available to assist you with questions regarding this incident, between the hours of 6:00 a.m. to 6:00 p.m. Mountain Time, Monday through Friday, excluding holidays. Please call the help line at 1-833-958-2107.

We thank you for your understanding deeply regret any worry or inconvenience that this may cause.

Very truly yours,

A handwritten signature in black ink, appearing to read 'RB' followed by a long horizontal stroke.

Brian Bosse
Partner
HBL CPAs, P.C.
5470 E Broadway Blvd
Tucson, AZ 85711

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL 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 credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. 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).

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 1-877-322-8228, 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 also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
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 Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. 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. 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>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This 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. 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.

Internal Revenue Service Identity Protection PIN (IP PIN): You may also obtain an Identity Protection PIN (IP PIN) from the Internal Revenue Service, a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification 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. Even though you may not have a filing requirement, an IP PIN still protects your account. If you do not already have an IP PIN, you may get an IP PIN as a proactive step to protect yourself from tax-related identity theft either online, by paper application or in-person. Information about the IP PIN program can be found here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

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.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
<https://www.marylandattorneygeneral.gov/>
1-888-743-0023

New York Attorney General

Bureau of Internet and
Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

**North Carolina Attorney
General**
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

**Washington D.C. Attorney
General**
441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include 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; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>