



Michael Christopher, Partner
Cybersecurity & Data Privacy Team
2029 Century Park East, Suite 1100
Los Angeles, CA 90067
mchristopher@constangy.com
Direct: 310.912.6183
Mobile: 949-322-8874

January 24, 2025

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: Notice of Data Security Incident

To Whom It May Concern:

Constangy, Brooks, Smith & Prophete, LLP represents Black, Bashor & Porsch, LLP ("BBP"), a company based in Sharon, Pennsylvania, 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.

1. What Happened

On December 11, 2024, BBP discovered unusual activity in its digital environment. Upon discovering this activity, BBP immediately took steps to secure the network and launched an investigation, aided by independent cybersecurity experts, to determine what happened and whether sensitive information may have been affected. As a result of the investigation, BBP learned that an unauthorized actor acquired certain files and data stored within its systems. Upon learning this, BBP launched a comprehensive review of all potentially affected information to identify any personal information that could have possibly been acquired. Following the completion of this comprehensive review, BBP confirmed on January 9, 2025, that certain personal information may have been involved in the incident. Since that time, BBP has been working to gather contact information for individuals and prepare notification to all affected individuals of this incident.

2. Number of Maryland Residents Notified and Type of Information

On January 24, 2025, BBP began notifying 5 Maryland residents of this data security incident via U.S. First-Class Mail. The data sets affected by this incident included individuals' names, and Social Security numbers. A sample copy of the notification letter sent to potentially impacted individuals known at this time is included with this correspondence.

3. Steps Taken Relating to the Incident

BBP has implemented additional security measures in an effort to prevent a similar incident from occurring in the future. Further, as referenced in the sample consumer notification letter, BBP has offered notified individuals 12 months of complimentary services through Identity Defense Complete, which includes credit monitoring, \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services.

January 24, 2025

Page 2

4. Contact Information

BBP remains dedicated to protecting the information in its possession. If you have any questions or need additional information, please contact me.

Very truly yours,

A handwritten signature in blue ink, appearing to read "MC" or "Michael Christopher", written over a light blue horizontal line.

Michael Christopher
CONSTANGY, BROOKS, SMITH & PROPHETE, LLP

Enclosure: Sample Notification Letter

Black, Bashor & Porsch, LLP
CERTIFIED PUBLIC ACCOUNTANTS

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

To Enroll, Please Visit:

app.identitydefense.com/enrollment/activate/bbp

Enrollment Code: <<Activation Code>>

Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<City>>, <<State>> <<Zip>>

<<Country>>

***Postal IMB Barcode

<<Date>>

Subject: Notice of Data Security Incident

Dear <<Full Name>>:

I am writing to inform you of a recent data security incident that may have affected your personal information. Black, Bashor & Porsch, LLP (“BBP”) takes the privacy and security of all information within its possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your personal information.

What Happened. On December 11, 2024, we discovered unusual activity in our digital environment. Upon discovering this activity, we immediately took steps to secure the network and launched an investigation, aided by independent cybersecurity experts, to determine what happened and whether sensitive information may have been affected. As a result of the investigation, we learned that an unauthorized actor acquired certain files and data stored within our systems. Upon learning this, we launched a comprehensive review of all potentially affected information to identify any personal information that could have possibly been acquired. Following the completion of this comprehensive review, we confirmed on January 9, 2025, that your personal information may have been involved in the incident. Since that time, we have been working to gather contact information for individuals and prepare notification to all affected individuals of this incident.

What Information Was Involved. Following our review of the contents of the impacted data, on January 9, 2025, we determined that your name and Social Security number were included. We emphasize that we have no evidence of any actual or attempted misuse of this information.

What We Are Doing. As soon as we discovered this incident, we took measures to further secure our network and enlisted outside cybersecurity experts to conduct a forensic investigation. We have also implemented additional security measures to help reduce the risk of a similar incident occurring in the future. In addition, we are notifying you of this event and providing resources you can utilize to help protect your information.

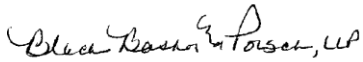
Out of an abundance of caution, we are offering identity theft protection services through Identity Defense. Identity Defense identity protection services include <<12/24>> months of credit monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, Identity Defense will help you resolve issues if your identity is compromised.

What You Can Do. We encourage you to enroll in free identity protection services by going to app.identitydefense.com/enrollment/activate/bbp. If you need assistance with the enrollment process or have questions regarding Identity Defense, please call Identity Defense directly at 1-866-622-9303. Your Activation Code to enroll is <<Activation Code>>. Please note the deadline to enroll is <<Enrollment Deadline>>. We also recommend that you review the guidance included with this letter about how to protect your information.

We also recommend that you create an Identity Protection PIN (IP PIN), which is a six-digit number that prevents someone else from filing a tax return using your Social Security number (SSN) or Individual Taxpayer Identification Number (ITIN). The IP PIN is known only to you and the IRS. It helps us 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. Please go to <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin> for information as to how to create an IP PIN.

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 888-754-0802 Monday through Friday from 9:00 a.m. to 9:00 p.m., Eastern Time. We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience this may cause.

Sincerely,

A handwritten signature in cursive script that reads "Black, Bashor & Porsch, LLP".

Black, Bashor & Porsch, LLP

Steps You Can Take to Help Protect Your 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 (the “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 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 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.

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
877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
www.marylandattorneygeneral.gov/Pages/CPD
888-743-0023

New York Attorney General

The Capitol
Albany, NY 12224
800-771-7755
ag.ny.gov

**Rhode Island Attorney
General**

150 South Main Street
Providence, RI 02903
www.riag.ri.gov
401-274-4400

Iowa Attorney General

1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
888-777-4590

**NY Bureau of Internet and
Technology**

28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212.416.8433

Washington D.C. Attorney**General**

400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov/consumer-
protection
202-442-9828

NC Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov/protectingconsumers/
877-566-7226

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 www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.