



James M. Paulino, Esq.
Innovation Square
100 South Clinton Ave., Suite 1620
Rochester, NY 14604
jpaulino@constangy.com
Mobile: 585.281.3000

April 19, 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
Tel: 207-626-8800
Email: breach.security@maine.gov

Re: Notice of Data Security Incident

Dear Attorney General Aaron Frey:

Constangy, Brooks, Smith and Prophete LLP (“Constangy”) represents Butler, Lavanceau & Sober, LLC (“BLS”) located at 10450 Shaker Drive, Suite 112, Columbia, Maryland 21046 in connection with an incident described in greater detail below. Please be advised BLS reserves all rights, claims and defenses in connection with this matter.

1. Nature of Incident

On February 20, 2024, BLS experienced a network disruption and initiated an investigation to determine the full nature and scope of the incident. The investigation determined that certain files may have been accessed and/or acquired without authorization on February 20, 2024. After a thorough review of those files, BLS determined that personal information was identified as being contained within the potentially affected data. BLS conducted a thorough review of the affected data to identify any personal information that may have been involved and worked diligently to validate the results and confirm addresses of the potentially impacted individuals. This process concluded on March 21, 2024, after which BLS worked diligently to arrange for written notice of this event.

The information potentially involved for Maine residents varied by individual and may include the following: first and last name as well as Social Security number, driver’s license number, and limited medical/health information.

2. Number of Maine Residents Affected

BLS notified seven (7) Maine residents of the incident via U.S. mail on April 17, 2024. A sample

copy of the notification letter is included with this correspondence as *Exhibit A*.

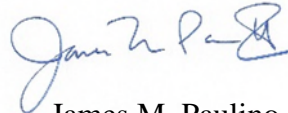
3. Steps Taken Relating to The Incident

Upon discovering the issue, BLS took the steps described above. In addition, BLS is offering individuals complimentary credit monitoring and identity protection services through Identity Defense. These services include 12 months of credit monitoring, identity protection, and fully managed identity theft recovery services. With this protection, Identity Defense will help them resolve issues if their identity is affected.

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.

Sincerely,

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

James M. Paulino, Esq.
Partner

Encl: Consumer notification letter template: Exhibit A.

Exhibit A



Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

<<First Name>> <<Last Name>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip Code>>
<<Country>>

<<Date>>

<<Variable data 1>>

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

I am writing to inform you of a recent incident that may have affected your personal information. At Butler, Lavanceau, & Sober, LLC (“BLS”) we take the privacy and security of personal information very seriously. This is why we are informing you of the incident, providing you with steps you can take to protect your personal information, and offering you complimentary credit monitoring and identity protection services; enrollment instructions are on the following pages.

What Happened. On February 20, 2024, BLS experienced a network disruption and initiated an investigation to determine the full nature and scope of the incident. The investigation determined that certain files may have been accessed and/or acquired without authorization on February 20, 2024. After a thorough review of those files, on or about March 21, 2024, we determined that some of your personal information was identified as being contained within the potentially affected data.

What Information Was Involved. The information may have included your name, Social Security number, driver’s license number, and limited medical/health information if it was provided to our office.

What We Are Doing. As soon BLS discovered the incident we took the steps described above and implemented measures to enhance network security and minimize the risk of a similar incident occurring in the future. We notified the Federal Bureau of Investigation and will provide whatever cooperation may be necessary to hold the perpetrators accountable.

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 “opt-in” program requiring specific coordination with the IRS prior to e-filing. We are also 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 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>.

We are also offering you complimentary credit monitoring and identity protection services through Identity Defense, a leader in consumer identity protection. These services include <<CM Duration>> months of credit monitoring, identity protection through Identity Defense.

What You Can Do. You can follow the recommendations on the following page to help protect your personal information and enroll in the complementary services offered to you through Identity Defense.

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 1-888-837-1216 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,

Butler, Lavanceau, & Sober, LLC

Butler, Lavanceau, & Sober, LLC
10450 Shaker Drive, Suite 112 Columbia, Maryland 21046

STEPS YOU CAN TAKE TO PROTECT YOUR PERSONAL INFORMATION

Enroll in Credit Monitoring Services:

<<First Name>> <<Last name>>
Activation Code: <<Activation Code>>
Enrollment Deadline: <<Enrollment Deadline>>

To enroll in Identity Defense, visit app.identitydefense.com/enrollment/activate/blsl

1. Enter your unique Activation Code <<**Activation Code**>>
Enter your Activation Code and click 'Redeem Code'.
2. Create Your Account
Enter your email address, create your password, and click 'Create Account'.
3. Register
Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.
4. Complete Activation
Click 'Continue to Dashboard' to finish enrolling.

If you do not enroll by <<Enrollment Deadline>>, you will not be able to take advantage of Identity Defense, so please enroll before the deadline. If you need assistance with the enrollment process or have questions regarding Identity Defense, please call Identity Defense directly at 1.866.622.9303.

*Service Term begins on the date of enrollment, provided that the enrollment takes place during the approved enrollment period.

**Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

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>.

STEPS YOU CAN TAKE TO PROTECT YOUR PERSONAL INFORMATION

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.

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>.

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
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/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf>.