Julie M. Hess, Partner
Cybersecurity & Data Privacy Team
1650 Market Street, 36th Floor
Philadelphia, Pennsylvania 19103
jhess@constangy.com
610.416.9236

November 18, 2025

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

Re: Notice of a Data Security Incident

Dear Attorney General Frey:

Constangy Brooks Smith & Prophete represents Murphy, Pearson, Bradley & Feeney, APC ("MPBF"), located in San Francisco, California, in connection with a data security incident described in greater detail below. The purpose of this letter is to notify you of the incident.

1. **Nature of the Security Incident**

On April 10, 2025, MPBF discovered suspicious activity on its network and promptly took steps to secure its environment and initiated an investigation of the matter. MPBF immediately engaged independent cybersecurity experts to assist with the process and determine the nature and scope of the incident. As a result of the investigation, MPBF learned that certain files may have been accessed or acquired without authorization. Following this confirmation, MPBF undertook a comprehensive review of those files and, on or about November 11, 2025, determined that personal information belonging to certain individuals was contained within the potentially impacted data. Please note that MPBF has no evidence of the misuse, or attempted misuse, of any potentially impacted information.

The data elements impacted by this incident vary by individual but may have included the following: Social Security number.

2. **Number of Maine Residents Affected**

MPBF notified 1 Maine residents of this incident via first class U.S. mail on November 18, 2025. A sample copy of the notification letter sent to impacted individuals is included with this correspondence.

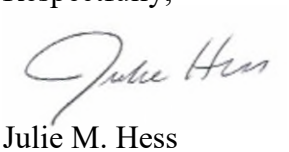
3. Steps Taken Relating to the Incident

MPBF has taken steps to prevent similar incidents from occurring in the future and is also offering complimentary identity protection services to all individuals notified of the incident.

4. Contact Information

MPBF remains dedicated to protecting the personal information in its possession. If you have any questions or need additional information, please do not hesitate to contact me directly by phone 610.416.9236 or email at jhess@constangy.com.

Respectfully,



Julie M. Hess
Constangy, Brooks, Smith & Prophete, LLP

Enc.: Sample Consumer Notification Letter

MURPHY | PEARSON
BRADLEY & FEENEY

<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>



<<Date>> (Format: Month Day, Year)

<<b2b_text_1 (Subject: Notice of Data Security Incident / Breach)>>

Dear <<First_name>> <<Last_name>>:

We are writing to inform you of a recent data security incident that may have affected your personal information. Murphy, Pearson, Bradley & Feeney, APC ("MPBF") 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, should you feel it necessary to do so.

What Happened. On April 10, 2025, we discovered suspicious activity on our network and promptly took steps to secure our environment and initiated an investigation of the matter. We engaged independent cybersecurity experts to assist with the process and determine the nature and scope of the incident. As a result of the investigation, we determined that certain files may have been accessed or acquired without authorization. Following this confirmation, we undertook a comprehensive review of those files and, on or about November 11, 2025, we determined that personal information belonging to certain individuals, including you, was contained within the potentially impacted data. Please note that we have no evidence of the misuse, or attempted misuse, of any potentially impacted information.

What Information Was Involved. The information may have included your name as well as your <<b2b_text_2 (Affected Regulated Data Sets)>>.

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

Although we have no evidence of the misuse of any information as a result of this incident, we are also offering you complimentary identity protection services through Kroll, a leader in consumer identity protection. These services include <<ServiceTerminMonths>> months of Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. The deadline to enroll in these services is <<b2b_text_6 (activation deadline)>>.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (activation deadline)>> to activate your identity monitoring services.

Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

What You Can Do. We urge you to always take steps to avoid identity theft and review the recommendations on the enclosed "Steps You Can Take to Help Protect Your Information" for more information. We also encourage you to enroll in the complimentary monitoring services being offered to you through Kroll by using the enrollment information provided. Please note, we are unable to enroll you in these services and you must do so on your own.

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 (844) 354-3825 Monday through Friday from 8:00 a.m. to 5:30 p.m. Central, excluding US holidays. We take your trust in us and this matter very seriously. Representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your information.

Please accept our sincere apologies for any worry or inconvenience this may cause.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft. To receive credit 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.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

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 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 2000
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

Oregon Attorney General
1162 Court St., NE
Salem, OR 97301
www.doj.state.or.us/consumer-protection
877-877-9392

California Attorney General
1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
800-952-5225

New York Attorney General
The Capitol
Albany, NY 12224
800-771-7755
ag.ny.gov

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

NY Bureau of Internet and Technology
28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212.416.8433

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.