

September 15, 2025

Via Portal Submission

Attorney General Aaron Frey
Office of the Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall Street, 6th Floor
Augusta, ME 04330
Email: breach.security@maine.gov

Re: Notice of Data Security Incident

To Whom it May Concern:

We represent Neubert, Pepe & Monteith, PC (“NP&M”), located at 195 Church Street, 13th Floor, New Haven, CT, 06510 and are writing to notify your office of an event that may affect the security of certain personal information relating to two (2) Maine residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, NP&M does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

1. Nature of the Data Event

On April 8, 2024, NP&M was alerted to potentially suspicious activity within its network. In response, NP&M took steps to secure its network and engaged cybersecurity experts to conduct an independent investigation. The investigation revealed that an unauthorized actor may have accessed certain files stored in its systems on March 1, 2024. NP&M then engaged an independent team to conduct a comprehensive review of all potentially affected data and, on June 10, 2025, it learned that certain personal information may have been involved. It then worked diligently to identify contact information necessary to notify potentially impacted individuals. This process was completed on September 9, 2025.

The information that could have been subject to unauthorized access and/or acquisition includes first and last name, as well as Social Security number and driver's license number.

2. Notice to Maine Residents

On September 15, 2025, NP&M provided written notice of this event to two (2) Maine residents.

3. Other Steps Taken and To Be Taken

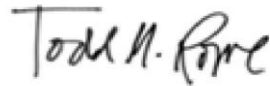
Upon becoming aware of the event, NP&M moved quickly to investigate and respond to the event, assess the security of its network, and identify potentially affected individuals. NP&M is also working to implement additional safeguards and training to its employees.

Additionally, NP&M is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected events of identity theft or fraud to their credit card company and/or bank. NP&M is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for events of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

4. Contact Information

If you have any questions or need additional information, please do not hesitate to contact me at trowe@constangy.com or 773.558.2363.

Sincerely,

A handwritten signature in black ink that reads "Todd N. Rowe". The signature is written in a cursive, slightly slanted style.

Todd Rowe of
CONSTANGY, BROOKS, SMITH & PROPHETE LLP

Enclosure: Consumer Notification Letter

Neubert, Pepe & Monteith, PC
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



September 12, 2025

Subject: Notice of Data Security Incident

Dear _____,

Neubert, Pepe & Monteith, PC (“NP&M”) is writing to inform you of a recent data security incident involving your personal information. At NP&M, we take the privacy and security of personal information very seriously. Please read this letter carefully as it contains information regarding the incident and steps you can take to help protect your personal information.

What Happened? On April 8, 2024, NP&M was alerted to potentially suspicious activity within its network. In response, NP&M took steps to secure its network and engaged cybersecurity experts to conduct an independent investigation. The investigation revealed that an unauthorized actor may have accessed certain files stored in our systems on March 1, 2024. We then engaged an independent team to conduct a comprehensive review of all potentially affected data and, on June 10, 2025, we learned that certain personal information may have been involved. We then worked diligently to identify contact information necessary to notify potentially impacted individuals. This process was completed on September 9, 2025.

What Information Was Involved? The information may have included your name and _____.

What We Are Doing. As soon as we discovered the incident, we took the steps described above and implemented additional security measures to minimize the risk of a similar incident occurring in the future. We also reported the incident to the FBI. In addition, we are offering you the opportunity to enroll for complimentary identity protection services through Cyberscout, a TransUnion company for _____ months.

What You Can Do. You can follow the recommendations on the following page to help protect your information. In addition, you can also enroll in TransUnion’s complimentary identity protection services. When prompted, please provide the unique code below to enroll in the services. The deadline to enroll is December 11, 2025.

For More Information. If you have any questions regarding the incident, please call **833-844-3171** between 8:00 A.M. to 8:00 P.M. Eastern Time, Monday through Friday (excluding holidays).

We take this event and the security of information in our care seriously. Please accept our sincere apologies and know that we deeply regret any concern or inconvenience that this may cause you.

Sincerely,

Neubert, Pepe & Monteith, PC

000010102G0400

P

Steps You Can Take to Help Protect Your Personal Information

Credit Monitoring Enrollment Instructions:

To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. 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. When prompted please provide the following unique code to receive services:

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
1-833-799-5355
www.transunion.com/get-credit-report

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. For TransUnion: www.transunion.com/fraud-alerts.

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. For TransUnion: www.transunion.com/credit-freeze.

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
www.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
www.ag.ny.gov

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



Kentucky Attorney General
700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
502-696-5300

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

The total number of Rhode Island residents receiving notification of this incident is 24.

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

00001020280000

P

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.

