David McMillan, Partner
Cybersecurity & Data Privacy Team
45 Main Street, Suite 206
Brooklyn, NY 11201
dmcmillan@constangy.com

October 6, 2025

VIA EMAIL
Attorney General John M. Formella
Office of the Attorney General
Consumer Protection & Antitrust Bureau
1 Granite Place South
Concord, NH 03301
DOJ-CPB@doj.nh.gov

Re: Notice of Data Security Incident

Dear Attorney General Formella:

Constangy, Brooks, Smith and Prophete LLP ("Constangy") represents Wear, Howell, Strickland, Quinn and Law, CPAs ("Wear Howell") in connection with an incident described in greater detail below. The purpose of this letter is to notify you, in accordance with New Hampshire data breach notification statute, that this incident may have affected the personal information of 10 New Hampshire residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. Wear Howell hereby reserves all rights and defenses in connection herewith.

1. Nature of Incident

On February 24, 2025, Wear Howell experienced an IT outage that disrupted access to certain local systems. After detecting and promptly containing the incident, Wear Howell launched an investigation with the support of external cybersecurity experts to learn more about the scope of the incident and any impact to data. Through that investigation, Wear Howell learned of information suggesting that an unknown actor gained unauthorized access to its network between February 11 and 19, 2025 and potentially acquired certain files, some of which may have contained individuals' personal information. Wear Howell then worked with additional experts to conduct a comprehensive review of the impacted data to determine what personal information was involved. On or about September 3, 2025, Wear Howell completed that review and learned that certain individuals' personal information may have been involved in connection with the incident.

The impacted information may have included the residents' names along with their Social Security numbers.

2. Number of New Hampshire residents affected

On October 6, 2025, Wear Howell notified 10 New Hampshire residents of the incident via first class U.S. mail. A sample copy of the notification letter is included with this correspondence.

3. Steps taken relating to the incident

In response to the incident, Wear Howell retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise. Wear Howell implemented additional security measures to further harden its environment in an effort to prevent a similar event from occurring

in the future. Wear Howell also reported this incident to federal law enforcement and is cooperating with the investigation.

Wear Howell is notifying the affected individuals and providing resources and steps individuals can take to help protect their information. In addition, Wear Howell is offering affected individuals complimentary monitoring and identity protection services through IDX, a data breach and recovery services expert. IDX's protection services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. IDX will also support a call center for at least 90 days to answer incident related questions.

4. Contact information

Wear Howell takes the privacy and security of all information in its possession very seriously. If you have any questions or need additional information, please do not hesitate to contact me at 718.614.8371 or dmcmillan@constangy.com.

Sincerely,

David McMillan of
CONSTANGY, BROOKS, SMITH & PROPHETE LLP

Encl.: Sample Consumer Notification Letter

Wear, Howell, Strickland, Quinn and Law, CPAs
Return Mail Processing Center
P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

October 6, 2025

Subject: Notice of Data <<Variable Text 1: Breach or Security Incident>>

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

The purpose of this communication is to notify you of a data security incident experienced by Wear, Howell, Strickland, Quinn and Law, CPAs ("Wear Howell") which may have affected your personal information. Wear Howell takes the privacy and security of all information in our possession very seriously. That is why we are notifying you of the event and providing you with resources to help protect your information. We encourage you to read this letter carefully and follow the steps outlined below.

What Happened? On February 24, 2025, we experienced an IT outage that disrupted access to certain local systems. After detecting and promptly containing the incident, we launched an investigation with the support of external cybersecurity experts to learn more about the scope of the incident and any impact to data. Through that investigation, we learned of information suggesting that an unknown actor gained unauthorized access to our network between February 11 and 19, 2025 and potentially acquired certain files, some of which may have contained individuals' personal information. We then worked with additional experts to conduct a comprehensive review of the impacted data to determine what personal information was involved. On or about September 3, 2025, Wear Howell completed that review and learned that your personal information may have been involved in connection with the incident which is the reason for this notification.

What Information Was Involved? We believe that the information involved in this incident may have included your name along with your <<Variable Text 2: Data Elements>>.

What We Are Doing. As soon as we discovered this incident, we launched an investigation and took steps to secure our IT environment, including by implementing enhanced security measures to help prevent a similar incident from occurring in the future. Wear Howell also notified the Federal Bureau of Investigation and will provide whatever cooperation is necessary to hold the perpetrator(s) of the incident accountable.

In addition, Wear Howell is offering you the opportunity to enroll in complimentary credit monitoring and identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: <<12/24>> months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. To enroll, please go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code <<ENROLLMENT>> or call (833) 831-8179. The deadline to enroll in these services is **January 6, 2026**.

What You Can Do. We encourage you to enroll in the complimentary credit protection services we are offering through IDX. With this protection, IDX can help you resolve issues if your identity is compromised. 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. If you have any questions regarding this incident or need assistance, IDX representatives are available for 90 days from the date of this letter between 8:00 am to 8:00 pm Central Time, Monday through Friday, excluding major U.S. holidays. If you have any questions, please call (833) 831-8179. IDX representatives are fully versed on this incident and can help answer questions you may have regarding the protection of your information.

Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Wear, Howell, Strickland, Quinn & Law, CPAs
1323 Stratford Road SE
Decatur, AL 35601

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	**Experian**	**TransUnion**
P.O. Box 105851	P.O. Box 9532	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-833-799-5355
www.equifax.com	www.experian.com	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	**Maryland Attorney General**	**Oregon Attorney General**
600 Pennsylvania Ave, NW	200 St. Paul Place	1162 Court St., NE
Washington, DC 20580	Baltimore, MD 21202	Salem, OR 97301
https://consumer.ftc.gov	www.marylandattorneygeneral.gov/Pages/CPD	www.doj.state.or.us/consumer-protection
877-438-4338	888-743-0023	877-877-9392

California Attorney General	**New York Attorney General**	**Rhode Island Attorney General**
1300 I Street	The Capitol	150 South Main Street
Sacramento, CA 95814	Albany, NY 12224	Providence, RI 02903
www.oag.ca.gov/privacy	https://ag.ny.gov	www.riag.ri.gov
800-952-5225	800-771-7755	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
https://oag.dc.gov/consumer-protection
202-442-9828

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

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
https://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.