David McMillan, Partner
Cybersecurity & Data Privacy Team
45 Main Street, Suite 206
Brooklyn, New York 11201
Telephone: 718.614.8371
Email: dmcmillan@constangy.com

October 30, 2025

VIA ELECTRONIC MAIL
Attorney General John Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
Email: DOJ-CPB@doj.nh.gov

Re: **Notice of Data Security Incident**

Dear Attorney General Formella:

Constangy, Brooks, Smith & Prophete, LLP ("Constangy") represents SC&H Group, Inc. ("SC&H") in connection with a data security incident described in greater detail below. The purpose of this letter is to notify you of the impact to state residents in accordance with New Hampshire's data breach notification statute.

1. Nature of the Security Incident

In late September 2025, SC&H learned that certain files had been transferred outside of its network without authorization by an employee who was later terminated. As soon as SC&H discovered this, SC&H took prompt action to investigate and determine precisely what information may have been affected. Following a thorough review of the files, SC&H determined that certain individuals' personal information may have been involved in this incident. SC&H then took steps to notify impacted individuals of the incident as quickly as possible.

Please note that SC&H has no indication this information has been used for identity theft, financial fraud, or other malicious activity and believes the information was transferred for the sole purpose of pursuing business relationships.

2. Number of Affected New Hampshire Residents & Information Involved

The incident involved personal information for two (2) New Hampshire residents. The information included individuals' names, Social Security and / or Taxpayer ID numbers, and driver's license numbers.

3. Notification of Affected Individuals

On October 30, 2025, notification letters were mailed to affected individuals by U.S. Mail. The notification letter provides resources and steps individuals can take to help protect

their information. The notification letter also provides potentially impacted individuals with complimentary credit monitoring and identity protection services through IDX – a data breach and recovery services expert. These services include credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. A sample copy of the notification letter sent to the impacted individuals is included with this correspondence.

3. Steps Taken to Address the Incident

In response to the incident, SC&H immediately launched an investigation to determine precisely what files were transferred without authorization and to identify any individuals whose personal information may have been involved. SC&H also taken steps to minimize the risk of a similar incident occurring in the future. These steps include new and updated trainings on safeguarding confidential information and enhanced technology security protocols to further restrict access from unauthorized devices.

4. Contact Information

SC&H remains dedicated to protecting the information in its control. If you have any questions or need additional information, please do not hesitate to contact me at dmcmillan@constangy.com or 718.614.8371.

Sincerely,

David McMillan of
CONSTANGY, BROOKS, SMITH & PROPHETE LLP

Enclosure: Consumer Notification Letter

P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<MI>> <<Last Name>>
<<Address 1>> <<Address 2>>
<<City>> <<State>> <<Zip>>

Enrollment Code: <<XXXXXXXX>>
Enrollment Deadline: January 30, 2026

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://app.idx.us/account-creation/protect

October 30, 2025

RE: Notice of Data <<Variable Text - Breach or Security Incident>>

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

SC&H Group, Inc. ("SC&H") is notifying you of an incident we believe may have involved your personal information. We take the confidentiality and security of your information very seriously and are notifying you of this incident, the steps we are taking in response, and resources we are making available to you.

What Happened. A former member of our Wealth Management Team ended employment with SC&H in July 2025. In late September 2025, we learned that certain files were transferred outside of our network without authorization. As soon as we discovered this, we took prompt action to investigate and determine precisely what information may have been affected. Following a thorough review of the files, we determined that your personal information may have been involved in this incident. Please note that SC&H has no indication this information has been used for identity theft, financial fraud, or other malicious activity and believes the information was transferred for the sole purpose of pursuing business relationships. However, out of an abundance of caution and in the interest of transparency, we are notifying you of this incident and providing resources to assist.

What Information Was Involved. Based on our investigation, we believe that the files transferred without authorization contained your name as well as your <<Variable Text – Data Elements>>.

What We Are Doing. Upon discovering this incident, we immediately initiated steps to protect our clients' information and provide this notice to you. We are pursuing all available avenues to ensure that any copies of client information improperly transferred are secured and/or removed from unauthorized possession and are no longer at risk. In addition, to alleviate any concerns you may have, SC&H is offering you complimentary identity protection services through IDX, a leader in consumer identity protection. These services include 24 months of credit monitoring, dark web monitoring, a $1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. The deadline to enroll in these services is January 30, 2026.

What You Can Do. We encourage you to enroll in the complimentary services offered to you through IDX by using the enrollment code provided above. In addition, we have also included an informational pamphlet which contains other resources you may utilize to help protect your personal information.

For More Information. If you have any questions regarding this incident or need assistance enrolling in the IDX services, please call 1-833-788-9712 Monday through Friday between 9:00 am and 9:00 pm, Eastern Time.

We deeply regret that this incident occurred and any impact that it may cause.

Sincerely,

Pritpal Kalsi
Chief Executive Officer
SC&H Group, Inc.

Steps You Can Take to 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 (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 105788
Atlanta, GA 30348
1-888-378-4329
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-800-831-5614
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.

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
1-877-438-4338

Maryland Attorney General St. Paul Plaza
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
ag.ny.gov
1-212-416-8433 / 1-800-771-7755

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
riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
400 S 6th 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://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.