WOODRUFF SAWYER

50 California Street, Floor 12, San Francisco, CA 94111 415.391.2141

March 4, 2024

Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

RE: Notice Concerning Security Breach

To Whom It May Concern:

We are writing to notify you that Woodruff-Sawyer & Co. ("Woodruff Sawyer") has experienced a data security incident. On January 20, 2024, a Woodruff Sawyer executive was victimized by a "SIM swapping" attack. An unknown individual went to a mobile carrier's retail store and successfully convinced a store employee to transfer the phone number of one of our executives to another device. The unauthorized third party was then able to use our executive's phone number to reset the executive's work password and access some of our cloud systems. The unauthorized third party downloaded a subset of files accessible via the victim executive's work account.

We discovered this incident on the same day it occurred—January 20, 2024—and took prompt action to terminate the unauthorized access, secure our systems, and investigate the attack. We have determined that the unauthorized third party had access to our systems for less than one day. We engaged a third-party cybersecurity firm to support our investigation of this incident and notified the Federal Bureau of Investigation (FBI) on January 21, 2024. Since discovering this incident we have strengthened our technical security controls to better protect Woodruff and its employees from SIM swapping attacks.

After discovering this incident, we initiated a review of the files downloaded by the unauthorized third party. We first discovered the presence of personal information within those files on February 5, 2024. The affected personal information is data that we receive from Woodruff's corporate clients in connection with our provision of insurance brokerage and risk consulting services to those clients.

We are continuing to review the downloaded files and are providing notice to affected individuals and government agencies in accordance with applicable laws. As of the date of this letter, we have identified affected personal information of 13 residents of New Hampshire. We are commencing notifications to affected individuals on March 4, 2024. Notification letters to individuals, a copy of which we have included with this letter, include an offer of of complementary identity theft protection services through Experian's IdentityWorks product.

Please do not hesitate to contact me if you have any questions.

Sincerely,

Vysali Soundararajan
50 California Street, Floor 12
San Francisco, CA 94111

WOODRUFF SAWYER

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

March 4, 2024

K9430-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

NOTICE OF DATA BREACH

Dear Sample A. Sample,

We are writing to notify you of a data security incident that affects some personal information about you. Woodruff-Sawyer & Co. ("Woodruff Sawyer") received your personal information because we provide insurance brokerage and risk consulting services to [Client Name].

What Happened? On January 20, 2024, an unauthorized third party gained access to certain Woodruff Sawyer computer systems and downloaded a small subset of our files. We initially discovered this unauthorized access on the same day and immediately began taking actions to secure our systems and to investigate the activity. We have determined that the unauthorized access occurred through the use of "SIM swapping." An unknown individual went to a mobile carrier's retail store and successfully convinced a store employee to transfer the phone number of one of our executives to another device. The unauthorized third party was then able to use our executive's phone number to reset the executive's work password and access our systems.

After discovering this incident, we initiated a review of the files downloaded by the unauthorized third party. On or around February 5, 2024, we determined that the downloaded files included some personal information. In the course of reviewing those files, which we have done on an ongoing basis since February 5, we identified personal information about you. We have not received any indication that your personal information has been further misused.

What Information Was Involved? The affected personal information included your

What Are We Doing? We engaged outside cybersecurity experts to help with our investigation of and response to this incident. We also notified the Federal Bureau of Investigation (FBI) of this incident and are cooperating with the FBI investigation. Further, we have amended our security controls to make it more difficult for an unauthorized party to access our systems through SIM swapping.

To help protect your identity, we are offering complimentary membership to Experian's® IdentityWorks℠. This product provides you with identity detection and resolution of identity theft. Below is information from Experian about its IdentityWorks services.

To activate your membership and start monitoring your personal information please follow the steps below:

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **833-918-1256** by . Be prepared to provide engagement number as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **833-918-1256**. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

What Can You Do? We suggest that you review the "Further Steps and Contact List" information on the reverse side of this letter, which identifies additional steps to take to protect your information. If you have additional questions or concerns about this incident, please call **833-918-1256**.

We take all privacy and security incidents seriously. We regret any inconvenience this may cause you, and thank you for your understanding. Woodruff Sawyer will **NOT** send you any electronic communications regarding this incident and ask you to disclose any personal information.

Sincerely,
Woodruff Sawyer

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

FURTHER STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION AND CONTACT LIST

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: It is always good practice to remain vigilant for signs of identity theft or other misuse of your data 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 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 can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact each one of the three national credit reporting agencies (contact information below).

Fraud Alert: You may 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 90 days. 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: A security freeze 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. Under federal law, you may not be charged to place or remove a credit freeze.

Police Report: If you file a police report, you have the right to obtain a copy of it. Please note that our notification to you was not delayed by law enforcement.

Additional Free Resources on Identity Theft: You can obtain information from the consumer reporting agencies, FTC (https://www.identitytheft.gov/) or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the Federal Trade Commission or to the Attorney General in your state. You may want to contact your state Attorney General to obtain further information. Below is the contact information for the Attorneys General for residents of New York, North Carolina, Rhode Island, Oregon, the District of Columbia, and Maryland.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

New York Attorney General
Office of the Attorney General
The Capitol
Albany, NY 12224-0341
https://ag.ny.gov/
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
401-274-4400

Oregon Attorney General
100 SW Market Street
First Floor
Tilikum Room
Portland, OR 97201
https://www.doj.state.or.us/consumer-protection/
1-877-877-9392

Office of the Attorney General for the District of Columbia
400 6th Street NW
Washington, D.C. 20001
oag@dc.gov
https://oag.dc.gov/

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
https://www.marylandattorneygeneral.gov/
Main number: 410-576-6300
Toll-free: 1-888-743-0023
Consumer Hotline: 410-528-8662

Contact Information for Credit Reporting Agencies:

	Equifax	**Experian**	**TransUnion**
To obtain a copy of your credit report	P.O. Box 740241 Atlanta, GA 30374 (866) 349-5191 www.equifax.com	P.O. Box 4500 Allen, TX 75013 (888) 397-3742 www.experian.com	P.O. Box 1000 Chester, PA 19016 (800) 888-4213 www.transunion.com
To obtain a security freeze	PO Box 105788 Atlanta, GA 30348 (800) 685-1111 www.equifax.com/personal/credit-report-services	PO Box 9554 Allen, TX 75013 (888) 397-3742 www.experian.com/freeze/center.html	P.O. Box 2000 Chester, PA 19016 (888) 909-8872 www.transunion.com/credit-freeze
To place a fraud alert	P.O. Box 105069 Atlanta, GA 30348 (888) 766-0008 www.equifax.com/personal/credit-report-services	P.O. Box 2002 Allen, TX 75013 (888) 397-3742 www.experian.com/fraud/center.html	P.O. Box 2000 Chester, PA 19016 (800) 680-7289 www.transunion.com/fraud-victim-resource/place-fraud-alert