MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

1266 E. Main Street, Soundview Plaza,
Suite 700 R
Stamford, CT 06902

January 24, 2024

VIA E-MAIL

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301
E-mail: DOJ-CPB@doj.nh.gov

Re: Notice of Data Event

To Whom It May Concern:

We represent Sigrist, Cheek, Potter & Huyser, PLLC ("SCP&H") located at 8110 E. Cactus Road, Suite 110, Scottsdale, AZ 85260, and are writing to notify your office of an incident that may affect the security of certain personal information relating to two (2) New Hampshire residents. This letter may be supplemented if any significant facts are learned subsequent to its submission. By providing this notice, SCP&H does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On July 11, 2023, SCP&H identified suspicious activity within an employee's email account and a cloud-based data storage site used to store documents. SCPH immediately took steps to secure the email tenant and storage site and launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the incident. The investigation determined that there was unauthorized access to the SCP&H environment from June 6, 2023, to July 12, 2023. SCP&H undertook a thorough and comprehensive review of all data potentially impacted by this event as to identify what information was contained within the data and to whom that data relates. On or about January 4, 2024, SCP&H determined that information related to New Hampshire residents may have been impacted by this event.

The information that could have been subject to unauthorized access and/or acquisition includes

.

Notice to New Hampshire Residents

On or about January 24, 2024, SCP&H provided written notice of this incident to two (2) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, SCP&H moved quickly to investigate and respond to the incident, assess the security of SCP&H systems, and identify potentially affected individuals. Further, SCP&H notified federal law enforcement, the IRS, and state tax authorities regarding the event. SCP&H is also reporting this event to the three consumer reporting agencies, Equifax, Experian, and Transunion. SCP&H is also working to implement additional safeguards and training to its employees. SCP&H is providing access to credit monitoring and identity restoration services for , through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, SCP&H is providing impacted individuals with guidance on how to better protect against identity theft and fraud. SCP&H 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 incidents 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at .

Very truly yours,

Gregory J. Bautista of
MULLEN COUGHLIN LLC

GJB/gpm
Attachment

EXHIBIT A

Sigrist, Cheek, Potter & Huyser
Certified Public Accountants

Return Mail Processing
PO Box 999
Suwanee, GA 30024

1 1 1 **********AUTO**MIXED AADC 300
SAMPLE A. SAMPLE - Individual
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

January 24, 2024

NOTICE OF DATA [EXTRA2]

Dear Sample A. Sample:

Sigrist, Cheek, Potter & Huyser, PLLC ("SCP&H") writes to inform you of a recent cyber incident that may impact the privacy of some of your information. This notice provides you with information about the incident, our response, and steps you may take to further protect your information against identity theft and fraud, should you determine it is appropriate to do so.

What Happened? On July 11, 2023, SCP&H identified suspicious activity within an employee's email account and a cloud-based data storage site used to store documents. In response, we immediately took steps to secure our email tenant and storage site and launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the incident. The investigation determined that there was unauthorized access to our email tenant and storage site from June 6, 2023, to July 12, 2023. SCP&H undertook a thorough and comprehensive review of all data potentially impacted by this event to identify what information was contained within the data and to whom that data relates. This review concluded on January 4, 2024, and we determined that information related to you may have been impacted by this event.

What Information Was Involved? Based on the review of the data, we determined that your name and [Extra1] were potentially accessed by an unknown, unauthorized actor as a result of this incident.

What We Are Doing. SCP&H takes this incident and the security of information within our care very seriously. Upon discovery of this incident, we immediately launched an in-depth investigation to determine the full nature and scope of this incident and moved quickly to assess the security of our email accounts and notify potentially affected individuals. As part of our ongoing commitment to the privacy of information within our care, we are working to implement additional security measures to further protect against similar incidents in the future. Additionally, we notified federal law enforcement, the IRS, and state tax authorities of this event and we will also be notifying state regulators, as required.

As an added precaution, we are offering complimentary access to [Extra3] months of credit monitoring services through Experian. Instructions on how to enroll in these services are enclosed in the *Steps You Can Take to Help Protect Your Information.* You must enroll yourself in these services as we are unable to activate these services on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud for the next 12 to 24 months and to review your account statements and credit reports to detect errors or suspicious activity. You can find more information about obtaining a free copy of your credit report, protecting against potential identity theft and fraud, and other resources available to you in the enclosed *Steps You Can Take to Help Protect Your Information*. You may also enroll in the complimentary credit monitoring services available to you; detailed instructions for enrolling in these services are enclosed.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, or need assistance, please contact us at **833-918-4335**, Monday through Friday from 8 am – 8 pm Central (excluding major U.S. holidays). You can also write to Sigrist, Cheek, Potter, & Huyser, Attn: Incident Response, 8110 E. Cactus Road, Suite 110, Scottsdale, AZ 85260.

Sincerely,

Daren Sigrist

Managing Partner

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Monitoring Services

To help protect your identity, we are offering complimentary access to Experian IdentityWorks[SM] for [Extra3] months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. 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 from the date of the incident (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 Identity Restoration is available to you for [Extra3] 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.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary [Extra3]-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at . Be prepared to provide engagement number [Engagement Number] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR [Extra3]-MONTH 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 specialists 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.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* 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.

Monitor Your Accounts

File Your Tax Return. We encourage you to file your tax return as soon as possible, if you have not already done so. You can also contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to prevent a fraudulent tax return from being filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

You should also look to the information made available by the tax authority for your state of residence and any other state where you file a tax return. For a list of websites for each US state's tax authority, visit http://www.taxadmin.org/state-tax-agencies.

We advise you to remain vigilant against identity theft and fraud by reviewing all account statements and monitoring free credit reports. If you discover or suspect fraudulent activity involving your account, credit or debit card, we encourage you to promptly contact the issuing bank or relevant financial institution. The number to call for assistance is usually on the back of the card.

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.