MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

April 1, 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: Supplemental Notice of Data Event

To Whom It May Concern:

We continue to represent Aldrich Services LLP ("Aldrich Services") located at 680 Hawthorne Ave SE, Suite 140, Salem, Oregon 97301, and write on behalf of all operating Aldrich Services affiliated entities including, Aldrich Wealth, to supplement our preliminary notification provided to your office on January 5, 2024, and notify your office of a data event that may affect the security of certain personal information relating to one (1) New Hampshire resident. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Aldrich Services 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

Aldrich Services provides various services affiliated with its provision of tax, advisory, and consulting services to individuals and businesses including to and on behalf of its affiliated entity, Aldrich Wealth, and collects information to further such services.

As noted in our January 5, 2024 preliminary notification, on or about October 11, 2023, Aldrich Services identified suspicious login activity to one of its employee's email accounts. Aldrich Services promptly responded, taking steps to secure the email account, and initiated an internal investigation to learn more about the suspicious activity. Further, as part of its response, Aldrich Services engaged third-party forensic specialists to conduct a comprehensive investigation to

confirm the full nature and scope of the incident. The investigation determined that a single email account was accessed by an unauthorized individual between October 9 and October 12, 2023.

Given the unauthorized access to the one email account, Aldrich Services, with the assistance of third-party specialists, undertook a comprehensive review of the contents of the relevant email account in order to identify the information that was present and to whom it related for purposes of assessing potential notification obligations. Due to the nature of services Aldrich Services performs for its clients across its various affiliated entities, the detailed review of the in-scope information and corresponding correlation to the appropriate customer/affiliated entity was and remains a time-intensive process.

Although these review efforts are ongoing at this time, based on the preliminary information and review efforts to date, certain information related to a single New Hampshire resident was identified which may have been accessed within the email account. The information related to the one (1) New Hampshire resident includes

Notice to New Hampshire Resident

On or about April 1, 2024, Aldrich Services began providing written notice of this incident to potentially affected individuals, which includes approximately one (1) New Hampshire resident. Written notice is being provided in substantially the same form as the letter attached hereto as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering, Aldrich Services promptly took steps to confirm the security of its email environment, including changing the account password, and initiated a comprehensive investigation to determine the full nature and scope of the matter and to identify potentially affected individuals. Further, Aldrich Services promptly notified federal law enforcement regarding the matter. Moreover, as part of its ongoing commitment to the privacy and security of the information in its care, Aldrich Services is reviewing, and where necessary, enhancing its policies and procedures related to data security to reduce the likelihood of a similar matter in the future, and providing additional training to employees regarding data security. As an added measure, Aldrich Services is also providing access to credit monitoring services for , through Kroll, to individuals whose information was potentially affected by this incident, at no cost to these individuals.

Additionally, Aldrich Services is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Aldrich Services is also 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. Moreover, Aldrich Services is providing written notice of this matter to relevant regulatory authorities, as required, and to the major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

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

Very truly yours,

Julie Siebert-Johnson of
MULLEN COUGHLIN LLC

JSJ/ajl
Enclosure

EXHIBIT A

Aldrich Services LLP
680 Hawthorne Avenue SE, #140
Salem, OR 97301

<<Date>> (Format: Month Day, Year)

<<first_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1(subject line)>>

Dear <<first_name>> <<last_name>> <<suffix>>:

As the Chief Operating Officer of Aldrich Services, I am reaching out to notify you of a matter that may affect certain information related to you that we received in connection with our relationship with <<b2b_text_2(Aldrich Entity/Data Owner)>>. At Aldrich Services, we deeply value the trust you place in us and our partners to protect your information. Please be assured that we take this matter seriously, have been working diligently to investigate and respond, and are committed to protecting the information in our care. Although we have no evidence of any actual or attempted misuse of your personal information as a result of this matter, this letter provides information about the matter, our response, and steps you may take to help protect your information, should you feel it is appropriate to do so.

What Happened? After Aldrich Services identified unusual activity involving one of our employee's email accounts, we quickly took steps to secure the email account, confirm the security of our entire email environment, and initiated a comprehensive investigation to gather additional information. The investigation confirmed that an unauthorized individual accessed one email account between October 9 and October 12, 2023. Although the investigation could not confirm that any particular information within the email account was accessed, in an abundance of caution, we then undertook a thorough review of the contents of the email account to identify what information was present and to whom such information related.

The preliminary results of this review were completed on February 20, 2024, after which we worked to review our files, and where possible, confirm necessary address information for identified individuals to prepare for notification. Due to the wide-ranging nature of services Aldrich Services performs for and provides to its clients, the data review and customer correlation was a time-intensive process. Following the team's significant efforts, on <<b2b_text_3(Enrichment date)>>, we completed an initial correlation of identified individuals to <<b2b_text_2(Aldrich Entity/Data Owner)>> and finished the necessary address enrichment efforts. You are receiving this letter because we determined that certain information related to you was present in the one impacted email account and therefore accessible in connection with this matter.

What Information Was Involved? Our investigation identified the following information relating to you was present in the email account: <<b2b_text_4( )>>.

What We Are Doing. Again, please know we take this matter and the responsibility to maintain the confidentiality, privacy, and security of the information in our care very seriously. In response to the matter, we promptly took steps to secure the account, including by changing the password, and conducted a diligent investigation to confirm the security of our network and the full nature and scope of the matter. We also promptly notified federal law enforcement. Further, as part of our ongoing commitment to the privacy and the security of information in our care, we are taking steps including working toward implementing additional technical security measures designed to reduce the likelihood of a future similar incident. We also plan to review, and where necessary, enhance our existing data privacy policies and procedures, and provide additional training to employees regarding the importance of safeguarding data to reduce the likelihood of a future similar event. We are also notifying relevant state and federal regulatory authorities, as required.

As an added measure to help protect your information and hopefully give you peace of mind, we are offering you access to of identity theft monitoring services through Kroll at no cost to you. We encourage you to activate these services as we are unable to act on your behalf to do so. If you wish to activate these services, please follow the instructions included in the attached *Steps You Can Take to Help Protect Personal Information*.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors over the next . You should report any suspicious charges to your credit/debit card or to the bank that issued the card or to the credit card company, as appropriate. You can also enroll to receive complimentary monitoring services that we are offering to you. Please also review the attached *Steps You Can Take to Help Protect Personal Information* for additional information and resources.

In addition, you can get a six-digit Identity Protection PIN (IP PIN) from the IRS to help protect against tax-related identity theft. An IP PIN helps the IRS verify your identity when filing an electronic or paper tax return. An IP PIN is valid for one calendar year and a new one is issued annually. For more information, including how to get an IP PIN, please visit: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

For More Information. We understand that you may have questions that are not addressed in this letter. If you have additional questions or concerns, please call our dedicated assistance line at xxx-xxx-xxxx, which is available 6:00 am to 3:30 pm Pacific Time, Monday through Friday excluding major U.S. holidays.

We want to reaffirm our unwavering commitment to your privacy and security, and sincerely regret any inconvenience or concern this may cause you.

Sincerely,

Josh Axelrod
Chief Operating Officer
Aldrich Services LLP

Steps You Can Take To Help Protect Personal Information

Activate Identity Monitoring Services

As an added measure, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people. Your identity monitoring services[1] include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

How to Activate Your Minor Monitoring Services

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.
You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.
Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Monitor Your Accounts

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 1-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 your 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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/. Aldrich Services is located at 680 Hawthorne Avenue SE, Suite 140, Salem, Oregon 97301.

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.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There is/are approximately # Rhode Island residents that may be impacted by this event.