MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

19109 West Catawba Avenue, Suite 200
Cornelius, NC 28031

February 10, 2023

VIA U.S. MAIL

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

Re: Notice of Data Event

To Whom It May Concern:

We represent Gries Financial Partners ("GFP") located at 1801 E. 9th St., Ste 1600, Cleveland, Ohio 44114. We are writing to notify your office of an incident 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 after its submission. By providing this notice, GFP 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 October 12, 2022, GFP became aware of unusual activity affecting two employees' email accounts. Upon discovery, GFP secured the accounts and commenced an investigation to understand the nature and scope of the incident. Through those efforts, GFP learned that additional email accounts used by its employees were subject to intermittent unauthorized access between September 8 and October 11, 2022, and that certain data housed in those accounts was accessible and potentially viewed. GFP initiated a comprehensive review to identify the types of potentially affected data in the accounts and to whom such data related. On January 6, 2023, GFP completed the review and identified that one (1) New Hampshire residents may be affected by the incident. GFP then worked to confirm contact information for potentially affected individuals so that it could effectuate direct notifications to those individuals as quickly as possible.

The information accessible in one or more of the email accounts and therefore potentially affected may include the following data types related to New Hampshire residents: name, address, financial

account information, Social Security number, and driver's license or other government identification number.

Notice to New Hampshire Residents

On or about February 10, 2023, GFP provided written notice of this incident to one (1) New Hampshire resident. Written notice is being provided in substantially the same form as the letter included herewith as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the incident, GFP moved quickly to investigate and respond, assess the security of GFP systems, and identify potentially affected individuals. Further, GFP notified federal law enforcement regarding the incident. GFP enhanced its email security protocols to further detect and respond to anomalous activity. GFP is also reviewing existing policies and procedures and implementing appropriate changes to reduce the likelihood of a similar future incident. As an added precaution, GFP is providing potentially affected individuals with access to complimentary credit monitoring services for two (2) years, through Kroll.

Additionally, GFP is providing potentially impacted individuals with guidance on how to protect their personal information. Specifically, GFP 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.

Gries is providing written notice of this incident to relevant state and federal regulators as necessary.

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,

Matthew V. Toldero of
MULLEN COUGHLIN LLC

MVT/dtg
Enclosure

EXHIBIT A

Gries Financial Partners

1801 E. 9th Street, Suite 1600
Cleveland, OH 44114
P: 216-861-1148
gries.com

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

<<Date>>

[UPDATE ON OCTOBER SECURITY INCIDENT] / [NOTICE OF DATA BREACH]

Dear <<Name 1>> <<Name 2>>:

Gries Financial Partners ("GFP") is writing in follow-up to our prior communications regarding an email security incident.

In accordance with our commitment to information privacy and security, we worked with third-party cybersecurity specialists to complete a thorough investigation into the incident. As indicated in prior communications, this letter is to notify you that the incident may impact the privacy of some of your information.

In response to the incident, we took immediate steps to protect our clients, including locking accounts. With this notice, we are providing details about the incident, steps we have taken in response, and resources available to help you better protect your information, should you feel such action is appropriate.

What Happened? On October 12, 2022, we became aware of unusual activity affecting two employees' email accounts. Upon discovery,
we secured the accounts and commenced an investigation to understand the nature and scope of the incident. Through those efforts, we learned that additional email accounts used by GFP employees were subject to intermittent unauthorized access between September 8 and October 11, 2022, and that certain data housed in those accounts was accessible and potentially viewed. We initiated a comprehensive review, with third-party cybersecurity specialists, to identify the types of potentially affected data and to whom such data related. On January 6, 2023, we assessed that personal information related to certain clients may have been included in the affected accounts.

What Information Was Involved? The information accessible in one or more of the email accounts, and therefore potentially affected, may include your name, address, financial account information, Social Security number, and driver's license information. **Please note that we have no evidence indicating that the unauthorized actor(s) accessed or viewed any specific information relating to you. We are providing this notice out of an abundance of caution.**

What Are We Doing? Safeguarding the privacy of information in our care and the security of our email environment is among our highest priorities. As indicated above, we promptly investigated the incident and took steps to evaluate system security. Specifically, we enhanced our email security protocols to further detect and respond to anomalous activity. More broadly, we are reviewing existing policies and procedures and implementing appropriate changes to reduce the likelihood of a similar future event.

As an added precaution, we are offering you access to complimentary identity monitoring services for 24 months through Kroll. More information about these services and instructions for enrollment may be found in the enclosed "Steps You Can Take to Protect Personal Information." Due to privacy restrictions, we are unable to act on your behalf, so if you would like to enroll in these services, please do so by following the instructions detailed on the following pages.

What You Can Do. Please review and consider the information and resources outlined in the below "Steps You Can Take to Help Protect Personal Information."

For More Information. If you have additional questions, please do not hesitate to contact your GFP client advisor or me directly. We appreciate your trust and apologize for the inconvenience.

Sincerely,

Jeffrey H. Palmer
President
Gries Financial Partners

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring

We have secured the services of Kroll to provide identity monitoring at no cost to you for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

How to Activate Your Identity Monitoring Services

1. You must activate your identity monitoring services by <<Enter Activation Deadline>>. Your Activation Code will not work after this date.
2. Visit Enroll.krollmonitoring.com/redeem to activate your identity monitoring services.
3. Provide Your Activation Code: <<Enter Activation Code>> and Your Verification ID: <<Enter Verification ID>>

Take Advantage of Your Identity Monitoring Services

You've been provided with access to the following services1 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 can help you determine if it's an indicator of identity theft.

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 can dig deep to uncover the scope of the identity theft, and then work to resolve it.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits, as applicable, and monitoring free credit reports for suspicious activity. Any questionable activity detected should be reported to the associated institution immediately.

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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one 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 your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide 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 you are a victim of identity theft.

Should you wish to place a credit freeze, 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
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

Internal Revenue Service Identity Protection PIN (IP PIN)

You may also obtain an Identity Protection PIN (IP PIN) from the Internal Revenue Service, a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. The IP PIN is known only to you and the IRS, and helps the IRS verify your identity when you file your electronic or paper tax return. Even though you may not have a filing requirement, an IP PIN still protects your account. If you do not already have an IP PIN, you may get an IP PIN as a proactive step to protect yourself from tax-related identity theft either online, by paper application or in-person. Information about the IP PIN program can be found here: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your 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, DC 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. GFP is located at 1801 E 9th St., Suite 1600 Cleveland, OH 44114.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your 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 your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You 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 you to review your 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.