Newman Dignan & Sheerar, Inc.
d/b/a NDS Wealth Advisors
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

[redacted]

October 9, 2024

Via First-Class Mail

Notice of Data Breach

Dear Dana Manchester:

Newman Dignan & Sheerar, Inc, d/b/a NDS Wealth Advisors ("NDS"), is writing to inform you of a security incident relating to certain personal information that you or a related person previously provided to us. Maintaining the security of your personal information is very important to us. Based on our investigation, we have no indication that information has been or will be used inappropriately, but we want to make you aware of the incident, the measures we have taken in response, and to provide details on steps that you can take to help protect your information. This notification was not delayed by law enforcement.

Why Does NDS Have My Personal Information?

NDS is a wealth management firm and also an investment advisor registered with the Securities and Exchange Commission. We provide investment, retirement, financial and estate planning services to individuals, organizations and trusts and estates. This work requires that we manage and interact with a variety of financial accounts and often involves collecting and processing personal information. For example, for tax reporting and compliance purposes, we receive and work with accountholder and beneficiary Social Security Numbers. In addition, to verify identity to us, as laws require, individuals submit copies of government-issued identification documents, such as drivers' licenses. NDS also on occasion processes payments for trust beneficiaries. During one or more of the above NDS business activities, we recorded some of your personal information.

What Happened?

On or about May 31, 2024, NDS discovered that the security of an email account assigned to one of our employees had been compromised by a cybercriminal. The cybercriminal exploited that unauthorized access to forge a revised wire transfer instruction, which NDS stopped from being implemented. We immediately launched an investigation, engaged a national cybersecurity forensic firm to assist in assessing the scope of the incident and took steps to mitigate the potential impact on all our clients. We have worked diligently to determine what happened and what information was involved in the incident. Unfortunately, these types of incidents are becoming increasingly common. Even organizations with the most sophisticated IT infrastructure are affected.

The third-party forensic investigation determined that the compromise of the NDS employee's email account had begun on or about May 28, 2024 and was terminated on May 31, 2024, the day that NDS discovered it. Thereafter, NDS retained electronic evidence specialists carefully to search the entire contents of the compromised email account for personal information.

What Information Was Involved?

Based on our investigation, the following personal information relating to you was available to and may have been acquired by the person who obtained unauthorized access to the above NDS email account between May 28 and May 31, 2024: your one or more financial account numbers, together with your name, physical address and other contact details. Again, however, we have no indication that your personal information has actually been misused.

What We Are Doing

We take this incident very seriously. Upon discovering the incident, we promptly launched an investigation, engaged a national cybersecurity firm to assist in assessing the scope of the incident and notified law enforcement. We have strengthened the security of our systems and procedures to reduce the risk of a future similar event.

In addition, out of an abundance of caution, we are providing you with access to **Single Bureau Credit Monitoring/ Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for 24 months from the date of enrollment when changes occur to your credit file. Alerts are sent to you the same day that the change or update takes place with the bureau. We also are providing you with **Proactive Fraud Assistance** to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted please provide the following unique code to receive services: **B646802675CC** In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

What You Can Do

Data frauds are not uncommon. We therefore recommend that you review the next few pages, which contain important information about additional steps you can take to safeguard your personal information, such as the implementation of fraud alerts and security freezes on your personal credit cards.

For More Information

We regret any inconvenience or concern this incident may cause you. Please call **(401) 445-0940** or email us (**client-assist@newmandignan.com)** with any questions you may have. Thank you for your consideration.

Sincerely,

William Newman, Principal
Newman Dignan & Sheerar, Inc.

Additional Important Information

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with
Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
TransUnion (https://www.transunion.com/fraud-alerts);
or Experian (https://www.experian.com/fraud/center.html).
A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
equifax.com/personal/credit-report-services/	experian.com/freeze/center.html	transunion.com/credit-freeze
1-800-349-9960	1-888-397-3742	1-888-909-8872

More information can also be obtained by contacting the Federal Trade Commission listed above.

Implementing an Identity Protection PIN (IP PIN) with the IRS:

To help protect against a fraudulent tax return being filed under your name, we recommend Implementing an Identity Protection PIN (IP PIN) with the IRS. An IP PIN is 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. It 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 don't already have an IP PIN, you may get an IP PIN as a proactive step to protect yourself from tax-related identity theft. If you want to request an IP PIN, please note: you must pass an identity verification process; and Spouses and dependents are eligible for an IP PIN if they can pass the identity verification process. The fastest way to receive an IP PIN is by using the online Get an IP PIN tool found at: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin. If you wish to get an IP PIN and you don't already have an account on IRS.gov, you must register to validate your identity.

Some items to consider when obtaining an IP PIN with the IRS:

- An IP PIN is valid for one calendar year.
- A new IP PIN is generated each year for your account.
- Logging back into the Get an IP PIN tool, will display your current IP PIN.
- An IP PIN must be used when filing any federal tax returns during the year including prior year returns.

For residents of *Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia, and Wyoming*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois*, *Iowa*, *Maryland*, *Missouri*, *North Carolina*, *Oregon*, and *West Virginia*:
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Vermont*: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

For residents of *New Mexico*: Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

For Residents of *Washington, D.C.*: You can obtain information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia at: 441 4th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft

For residents of *Massachusetts and Rhode Island*: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.