FMG LAW
Freeman Mathis & Gary LLP

60 State Street
Suite 600
Boston, MA 02109

www.fmglaw.com

Kirsten Patzer
Partner

Writer's Direct Access
617.963.5983

kirsten.patzer@fmglaw.com

August 3, 2022

VIA EMAIL
Maryland Attorney General
Idtheft@oag.state.md.us

RE: Notice of Data Event

Dear Sir or Madam:

We represent Nettworth Financial Group ("NFG"), a financial services firm located at 7284 West Palmetto Park Road Boca Raton, Florida. NFG recently learned that an unauthorized person may have had access to and/or acquired certain personal information of its current and former clients. NFG retained this firm and a cybersecurity forensics firm to investigate a security incident that occurred between September 18, 2021, and November 11, 2021, and while NFG cannot confirm that any clients' information was in fact accessed or acquired, NFG's investigation and review of the information contained on its network reveals that there was the potential for access and/or acquisition. This submission is, accordingly, made to ensure compliance with the Maryland data breach notification law, Md. Code Com. Law §14-3504 (2018), which requires notice to your office in the event of a breach in the security of personal information affecting residents of the State of Maryland.

NFG became aware of an intruder into an email account on their system. NFG's information technology managed service provider took immediate steps to eliminate access by the intruder and secure the network. NFG shortly thereafter began working with counsel and a third-party cybersecurity specialist to investigate the incident. The investigation revealed, on or about March 18, 2022, personal information respecting NFG's current and former clients was potentially accessed and/or acquired by an unauthorized actor between the dates of September 18, 2021 through November 11, 2021. A comprehensive review of the information revealed that six (6) residents of the State of Maryland were potentially affected. The types of personal information impacted include name, Social Security number, driver's license information and financial account information.

NFG notified all former and current employees whose information was potentially accessed and/or acquired. After providing this notification, NFG will provide notification to the six (6) residents of the State of Maryland affected by the incident. A sample copy of that notice is attached as Exhibit "A" for your records.

After discovering the incident, NFG undertook a secure, managed restoration of the account, had all passwords reset and implemented multi-factor authentication. NFG further engaged a third-party cybersecurity forensic firm to thoroughly investigate the incident. In addition, NFG is reviewing its existing security measures in place for enhancements to best prevent a similar incident from occurring in the future and encrypting personal information. NFG is also notifying other state regulators as necessary.

I believe this provides you with all information necessary for your purposes and to comply with Maryland law. However, if anything further is needed, please contact me directly.

Respectfully,

FREEMAN MATHIS & GARY, LLP

Kirsten Patzer

EXHIBIT A

Making Investments Make Sense

Jonathan Marc Beitler
Financial Advisor
7284 West Palmetto Park Road
Suite 202-S
Boca Raton, **FL 33433**
Office: (561) 447-8444
Toll Free: (866) 553-9015
Fax: (561) 235-5486
Email: jbeitler@nettworth.us
Web: www.nettworth.net/florida

June 29, 2022

«AddressBlock»

«GreetingLine»

At Nettworth Financial Group ("NFG"), we take the issue of privacy seriously. As part of that commitment, we are notifying you of a recent data security incident that may have affected your personal information. Please read this letter carefully.

What Happened

NFG recently learned that between September 18, 2021 and November 11, 2021, an unauthorized person gained access to an email account located on our system. We cannot confirm what information or documents, if any, were specifically accessed by the unauthorized person during that incident. However, because this email account contained documents with individuals' personal information, it is possible that the unauthorized person accessed or acquired that information. In an abundance of caution, we are now notifying potentially affected individuals.

What Information Was Involved

At this time, NFG cannot confirm that your personal information was in fact accessed, viewed or acquired. We also are not aware of any misuse of your information or disclosure of it by the unauthorized person involved in this incident. However, you are receiving this letter because, based on our investigation, there was the potential for unauthorized access to and/or acquisition of your personal information, including your full name, address, Social Security number, account numbers, and driver's license information.

What We Are Doing

We immediately undertook an investigation of the incident with the guidance and assistance of a third-party cybersecurity firm. We have worked to identify the scope of the incident and to ensure the security of our system and data. We immediately changed the password to the affected account and implemented multi-factor authentication to prevent future unauthorized access.

What You Can Do

In light of this incident, we recommend that you remain vigilant by reviewing and monitoring your account statements and credit reports. If you find any errors or unauthorized activity, you should contact your financial institution or call the number on the back of your payment card. You also may file a report with law enforcement, your state attorney general, and/or the Federal Trade Commission. In addition, please refer to the enclosed documentation which contains additional steps you may take to protect your information from misuse, including some information that may be specific to your state of residence.

For More Information

We are very sorry for any concern or inconvenience this incident has caused or may cause you. If you have any other questions or concerns that you would like to discuss, you may contact us at 866-553-9015.

Sincerely,
Jonathan Beitler
Jonathan Beitler

ADDITIONAL STEPS TO HELP PROTECT YOUR INFORMATION

Review personal account statements and credit reports. We recommend that you remain vigilant by reviewing personal account statements and monitoring credit reports to detect any errors or unauthorized activity. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call (877) 322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months. If you discover any suspicious items, you should report any incorrect information on your report to the credit reporting agency. The names and contact information for the credit reporting agencies are:

Equifax	Experian	TransUnion
1-866-766-0008	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com

Report suspected fraud. You have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You should report suspected incidents of identity theft to local law enforcement, your state's Attorney General, and/or the Federal Trade Commission.

Place Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. Starting September 21, 2018, when you place a fraud alert, it will last one year, instead of 90 days. Fraud alerts will still be free and identity theft victims can still get an extended fraud alert for seven years. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. To place a security freeze, contact the nationwide credit reporting agencies by phone or online. For more information, visit https://www.consumer.ftc.gov/articles/0275-place-fraud-alert.

Place a Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. Starting September 21, 2018, you can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too. To place a security freeze, contact the nationwide credit reporting agencies by phone or online. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee. Also, do not confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock. For more information, visit https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs.

Change Online Account Credentials. If the information involved in this incident included credentials used to access any of your online accounts, such as a username, password, PIN, or answer security question, you should to promptly change your username, password, PIN, security question and answer, or other access credentials and take other appropriate steps to protect all online accounts for which you use the same credentials.

Obtain additional information about the steps you can take to avoid identity theft from the following entities:

- **California Residents:** Visit the California Office of Privacy Protection, www.privacy.ca.gov, for additional information on protection against identity theft.
- **Iowa Residents:** Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov,(515) 281-5164.
- **Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, (502) 696-5300.
- **Maryland Residents:** Office of Attorney General of Maryland**,** Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, (888) 743-0023.
- **North Carolina Residents:** Office of the Attorney General of North Carolina**,** 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.com, (919) 716-6400.
- **Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us, (877) 877-9392.
- **Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, (401) 274-4400.
- **All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.ftc.gov, 1-877-IDTHEFT (438-4338).

Know Your Rights Under the Fair Credit Reporting Act. The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. You have certain rights under the FCRA, which you can read about by visiting https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf and https://www.consumer.ftc.gov/articles/0070-credit-and-your-consumer-rights. These rights include: (1) You must be told if information in your file has been used against you; (2) You have the right to know what is in your file (you “file disclosure”); (3) You have the right to ask for a credit score; (4) You have the right to dispute incomplete or inaccurate information; (5) Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (6) Consumer reporting agencies may not report outdated negative information; (7) Access to your file is limited to people with a valid need; (8) You must give your consent for reports to be provided to employers; (8) You may limit “prescreened” offers of credit and insurance you get based on information in your credit report; (9) You may seek damages from violators; and (10) identity theft victims and active duty military personnel have additional rights. For more information, visit www.ftc.gov/credit. States may enforce the FCRA, and many states have their own consumer reporting laws. In some cases, you may have more rights under state law. For more information, contact your state or local consumer protection agency or your state Attorney General.