Clark Hill

Melissa K. Ventrone
T (312) 360-2506
Email:mventrone@ClarkHill.com

Clark Hill
130 E. Randolph Street, Suite 3900
Chicago, Illinois 60601
T (312) 985-5900
F (312) 985-5999

November 4, 2022

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03302
attorneygeneral@doj.nh.gov

To Whom it May Concern:

We represent the Girard Financial Group L.L.C., d.b.a. G9 Financial ("G9 Financial") as Outside Counsel with respect to a data security incident involving the potential exposure of certain personally identifiable information ("PII") described in more detail below. G9 Financial, a financial planning group located in Millbury, MA, is committed to answering any questions you may have about the data security incident, its response, and steps taken to prevent a similar incident from occurring in the future.

1. Nature of security incident.

On April 25, 2022, G9 Financial learned of suspicious activity associated with one of their corporate email accounts. G9 Financial immediately started an internal investigation to determine what occurred and whether any data was accessed or exfiltrated. The investigation found unauthorized access to one account but was unable to determine whether any data was compromised. G9 Financial then hired a vendor to conduct an in-depth review of the email account to identify any personal information that may have been located in the account. This review was completed on September 30, 2022. From this review, it appears the information in the account may have included individuals' names, addresses, financial account information, Social Security numbers, and limited medical information.

2. Number of residents affected.

Twelve (12) New Hampshire residents may have been affected and were notified of the incident. A notification letter was sent to the potentially affected individuals on November 7, 2022. A copy of the form notification letter is enclosed.

3. Steps taken in response to the incident.

Since this incident, G9 Financial changed the password to the affected corporate email account and enabled multifactor authentication across all corporate email accounts. Additionally, impacted individuals were offered 12 months of credit monitoring and identity protection services through Cyberscout.

4. Contact Information

G9 Financial takes the security of the information in its control seriously and is committed to ensuring it is appropriately protected. If you have any questions or need additional information, please do not hesitate to contact me at mventrone@clarkhill.com or (312) 360-2506.

Sincerely,

CLARK HILL

Melissa K. Ventrone

cc: John F. Howard - jfhoward@clarkhill.com

G9 Financial
<<Return Address>>
<<City>>, <<State>> <<ZIP>>

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZIP>>

<<Date>>

Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>,

G9 Financial is writing to let you know about a data security incident that may have affected your personal information. We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this incident may cause you. This letter contains information about what occurred, steps you can take to protect your information, and resources we are making available to help you do so.

What happened?

On April 25, 2022 we discovered suspicious activity associated with one of our email accounts. We immediately started an internal investigation and hired an independent computer forensics firm to help with our investigation. The investigation found unauthorized access to one email account but was unable to determine if any information in the account was accessed. Out of an abundance of caution, we hired a vendor to do an in-depth review of the account to determine what personal information may have been present. This review was completed on September 30, 2022, at which point we identified that some of your personal information may have been located in the account in question.

While we have no evidence that your personal information compromised or misused we wanted to notify you about this incident and provide you with resources to protect yourself.

What information was impacted?

From the review, it appears that your name, address, <<Variable Text>> may have been impacted by this incident.

What we are doing:

We want to assure you that we have taken steps to prevent this kind of event from happening in the future. Since the incident, the passwords to the affected email account were changed and multifactor authentication was enabled across all G9 Financial email accounts.

In response to this incident, we are providing you access to the following services:

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday. Please call the help line 1-800-405-6108 and supply the fraud specialist with your unique code listed below. To extend these services, enrollment in the monitoring services described below is required.

* Services marked with an "*" require 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.

Additionally, 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 <<Length of service>> from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we 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 through Identity Force, a 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 **<<URL>>** and follow the instructions provided. When prompted please provide the following unique code to receive services: **<CODE HERE>** In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

What you can do:

It is always a good idea to remain vigilant and be on the look-out for evidence of identity theft or fraud, and to review your bank account and other financial statements as well as your credit reports for suspicious activity. We also encourage you to contact Cyberscout with any questions and to take full advantage of the Cyberscout service offering. Additional information about protecting your identity is included in this letter, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For more information:

If you have any questions or concerns, please call **1-800-405-6108** Monday through Friday from 8:00 am – 8:00 pm Eastern Time. Your trust is our top priority, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

Daniel F. Girard, Jr.
Girard Financial Group L.L.C.
d.b.a. G9 Financial

* Services marked with an "*" require 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.

RECOMMENDED STEPS TO HELP PROTECT YOUR INFORMATION

You've been provided with access to the following services from Cyberscout:

1. 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 Cyberscout fraud specialist, who can help you determine if it's an indicator of identity theft.

2. Fraud Consultation. You have unlimited access to consultation with a Cyberscout 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.

3. Identity Theft Restoration. If you become a victim of identity theft, an experienced Cyberscout 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.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. 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 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You should also know that 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 can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
P.O. Box 105069
Atlanta, GA 30348-5069

Equifax Credit Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-836-6351
www.equifax.com/personal/credit-report-services

Experian Fraud Reporting and Credit Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion Fraud Reporting
P.O. Box 2000
Chester, PA 19022-2000

TransUnion Credit Freeze
P.O. Box 160
Woodlyn, PA 19094
1-800-680-7289
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

* Services marked with an "*" require 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.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

Florida Residents: Office of the Attorney General, State of Florida, PL-01 The Capitol, Tallahassee, FL 32399-1050; Telephone: 1-800-435-7352; https://www.myfloridalegal.com

Massachusetts Residents: Massachusetts Office of the Attorney General, Data Privacy and Security Division, One Ashburton Place, Boston, MA 02108; Telephone: 1-617-727-8400

New Hampshire Residents: Office of the Attorney General, 33 Capitol St, Concord, NH 03301; Telephone: 1-603-271-3658

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

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Ohio Residents: The Office of the Attorney General, 30 E Broad St., 14th Floor, Columbus, OH 43215; Telephone: 1-800-282-0515; https://www.ohioattorneygeneral.gov

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. You have the right to obtain any police report filed in regard to this incident. There are 4 Rhode Island residents impacted by this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft

* Services marked with an "*" require 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.