



MULLEN
COUGHLIN_{LLC}

RECEIVED

MAR 20 2018

CONSUMER PROTECTION

Edward J. Finn
Office: 267-930-4776
Fax: 267-930-4771
Email: efinn@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

March 16, 2018

VIA U.S. MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Attorney General MacDonald:

We represent Clarfled Financial Advisors, 520 White Plains Road, Tarrytown, NY 10591, and are writing to notify your office of an incident that may affect the security of personal information relating to twenty-one (21) New Hampshire residents. The investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Clarfled Financial Advisors 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 March 9, 2018, Clarfled Financial Advisors learned from Charles Schwab & Company that an unknown person or persons gained access to the Schwab Advisor Center website using Clarfled Financial Advisors credentials. This website is used by Clarfled Financial Advisors to manage client accounts at Charles Schwab. The unauthorized person was able to acquire certain information related to the affected individuals from the website on or around February 22, 2018 and February 23, 2018. Charles Schwab had previously notified Clarfled on February 26, 2018, that limited information for 7 individuals, like account balances, and possibly some other information, was viewed. However, on March 9, Schwab reported that names, Social Security numbers, and account numbers were acquired by unauthorized actors for a larger number of clients beyond the 7 individuals originally provided. Based on the investigation to date, no funds or positions were dispersed from client accounts nor were any trades executed. The unauthorized actor only had “view-only” access so he or she did not have ability to move money, initiate

transactions or manipulate data. Clarfeld Financial Advisors has been working tirelessly to investigate and to mitigate the impact of the attack.

Notice to New Hampshire Residents

On March 16, 2018, Clarfeld Financial Advisors provided written notice to its affected clients via first class mail. A copy of this notice is attached here as **Exhibit A**. The notice included twenty-one (21) New Hampshire residents.

Other Steps Taken and to Be Taken

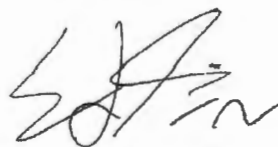
Upon discovering the fraudulent nature of the email, Clarfeld Financial Advisors moved quickly to identify those that may be affected, to put in place resources to assist them and to provide them with notice of this incident. Additionally, Clarfeld Financial Advisors will be working with forensic investigators to verify the nature and scope of the incident.

Clarfeld Financial Advisors is providing all potentially affected individuals access to 2 free years of credit and identity monitoring services, including identity restoration services, through AllClear ID, and has established a dedicated hotline for potentially affected individuals to contact with questions or concerns regarding this incident. Additionally, Clarfeld Financial Advisors is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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. Clarfeld Financial Advisors is also providing written notice of this incident to other state 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 267-930-4776.

Very truly yours,



Edward J. Finn of
MULLEN COUGHLIN LLC

EXHIBIT A

Date

Client Name/Address

Re: Notice of Data Breach

Dear Mr. Smith:

At Clarfeld Financial Advisors (CFA), protecting the security of the information in our possession is a responsibility we take very seriously. We are writing to notify you of a data security incident with your Charles Schwab & Company (Schwab) account that may have exposed some of your personal information. This letter explains the incident and steps CFA has undertaken to address it. In addition, we will provide guidance on what you can do to protect your personal information.

I. What Happened

On March 9, 2018, CFA learned from Schwab that an unknown person or persons gained access to the Schwab Advisor Center website using CFA credentials. This website is used by CFA to manage your account at Schwab. The unauthorized person may have been able to acquire certain information related to you from the Schwab website on or around February 22nd and 23rd, 2018.

II. What Information Was Involved

The information acquired included your name, Social Security number, address, and Schwab account number. Account values, balances and investment positions were not viewed, nor were dates of birth, passwords or login information. CFA and Schwab have found no evidence of any additional unauthorized access to your account. Based on the investigation to date, no funds or positions were disbursed from your account, nor were any trades executed in your account during the intrusion as the intruder had “view-only” access and had no ability to move money, initiate transactions or manipulate your data.

III. What We are Doing

Schwab Security Administration Center identified the unauthorized access and deactivated the intruder’s compromised credentials. Schwab communicated the incident to CFA, and we are conducting a review of our systems and processes, assisted by outside cybersecurity experts, to learn the cause of this intrusion, and if necessary, to identify additional steps that can be taken to help prevent this type of incident from happening again. So far, we have found no evidence whatsoever that our internal systems have been compromised.

As an added precaution, we have arranged to have AllClear ID protect your identity for 24 months at no cost to you. The following identity protection services start on the date of this notice and are available to you at any time during the next 24 months.

AllClear Identity Repair:

This service is available to you with no enrollment fees required. If a problem should arise, call 1-866-979-2595 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Fraud Alerts with Credit Monitoring:

This service offers the ability to set, renew, and remove 90-day fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, an annual credit score and credit report, and a \$1 million identity theft insurance policy. For a child under 18 years old, AllClear ID ChildScan identifies acts of fraud against children by searching thousands of public databases for use of your child's information. To enroll in this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-866-979-2595 using the following redemption code: {RedemptionCode}. Please note: following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may also be required in order to activate your monitoring options.

Further, Schwab is offering our clients access to a client "token" for an additional layer of security protection; the ability to suspend all online access to your account or lock it down permanently; voice identification services; and/or verbal passwords for account access. If appropriate, upon your instruction, CFA and Schwab can close an account that possibly was subject to this unauthorized access.

IV. What You Can Do

In addition to enrolling in Identity Theft Protection and credit file monitoring, please see the "Steps You Can Take to Protect Your Information" insert provided with this notice. This information provides additional steps you can take, including how to obtain a free copy of your credit report and place a fraud alert and/or credit freeze on your credit report. In addition, please monitor your account statements and report any unauthorized changes to CFA immediately.

V. For more Information

We completely understand that this is frustrating and aggravating, and for this we truly apologize. CFA is very much committed to ensuring that all client personal and account information is protected. If you have additional questions or require further assistance, please feel free to call me at 914-846-0122 or our Director of Investment Operations, Anthony Schembri, at 914-846-0117 and we will assist you.

Sincerely,

Joy Soodik
Senior Managing Director & Chief Compliance Officer

Enclosure

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

The following information is provided in accordance with certain state legal requirements.

Monitor Your Accounts

Credit Reports. 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. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Fraud Alerts. At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below:

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
800-680-7289
www.transunion.com

Security Freeze. You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. Fees vary based on where you live, but commonly range from \$3 to \$15. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788

Experian Security Freeze
P.O. Box 9554

TransUnion
P.O. Box 2000

Atlanta, GA 30348
1-800-685-1111
www.freeze.equifax.com

Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/

Chester, PA 19016
1-888-909-8872
freeze.transunion.com

Review of Account Statements Regularly. We recommend that you closely monitor your banking and credit account statements for suspicious activity on your existing accounts. You should remain vigilant by attentively monitoring your credit reports and account statements for indications of fraud and/or theft, including identity theft.

Additional Information. You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission can 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 encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be promptly reported to law enforcement, the Federal Trade Commission, and your state Attorney General. 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 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. This notice has not been delayed as the result of a law enforcement investigation.

For Maryland residents, the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us.

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 agencies 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 North Carolina residents, the Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov.

For Rhode Island residents, the Attorney General can be contacted by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at www.riag.ri.gov. A total of 7 Rhode Island residents may be impacted by this incident.