BRIAN MIDDLEBROOK
BMIDDLEBROOK@GRSM.COM

GORDON&REES
SCULLY MANSUKHANI

ATTORNEYS AT LAW
1 BATTERY PARK PLAZA, 28TH FLOOR
NEW YORK, NY 10004
WWW.GRSM.COM

November 6, 2018

VIA ELECTRONIC MAIL (ATTORNEYGENERAL@DOJ.NH.GOV)
Gordon J. MacDonald, Attorney General
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notification of Data Security Incident
Our File No: 1166796

Dear Attorney General MacDonald:

Our client, HC Financial Advisors, Inc. ("HC Financial"), a financial planning and investment management firm located in Lafayette, California, understands the importance of protecting the personal information provided by its customers and is making this notification to your Office pursuant to N.H. Rev. Stat. §§ 359-C:19 – C:21.

On August 2, 2018, one of the principals of HC Financial identified irregularities in the MS Office 365 environment. HC Financial immediately requested that its IT consultant evaluate these irregularities and signs of unauthorized access to the network were identified. Thereafter, the consultant immediately terminated the unauthorized access and confirmed that the network was secure. While the nature of the intrusion did not suggest that any specific private information was accessed, in an abundance of caution, HC Financial undertook further investigative efforts to identify any specific individuals whose personal information may have been compromised.

The forensic investigation was inconclusive as to the cause or origin of the system compromise, nor was there evidence of specific data acquisition within the mailbox. As a result, and in continuing to exhaust investigative efforts, a full and time consuming analysis of the impacted mailbox was performed. Specifically, the investigation identified the personal information of 107 individuals within this mailbox, including information such as social security numbers, tax identification numbers, passport numbers, and drivers' license numbers. Again, the information was available and it cannot be ruled out that it was not acquired, but there is no evidence of acquisition. HC Financial does not have any reason to believe that this incident will result in harm to the individuals whose personal information may have been acquired or accessed as a result of this incident.

Nonetheless, in an abundance of caution, HC Financial will be providing written notification on November 9, 2018 to 107 individuals, including one (1) New Hampshire resident pursuant to N.H. Rev. Stat. §§ 359-C:19 – C:21, indicating the above. A sample copy of the

notification to the New Hampshire resident is attached. As noted in the attachment, HC Financial has included in the notification an offer to provide twenty-four months of three bureau credit monitoring services to the affected New Hampshire resident, as well as all of the 107 individuals notified as a result of this incident.

HC Financial is continuing to work closely with leading security experts to identity and implement measures to further strengthen the security of its system to help prevent this from happening in the future.

Best regards,

GORDON REES SCULLY MANSUKHANI, LLP

/s/ Brian Middlebrook

Brian E. Middlebrook, Esq.

Enclosures

CC: [redacted]

FINANCIAL ADVISORS, INC.
Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>>:

HC Financial Advisors, Inc. ("HC Financial") values your business and understands the importance of protecting your personal information. We are writing to inform you that we recently identified and addressed a security incident that may have involved your personal information. This notice describes the incident, outlines the measures we have taken in response, and advises you on steps you can take to further protect your information.

What Happened?

On August 3, 2018, one of the principals of HC Financial identified irregularities in the MS Office 365 environment. HC Financial immediately requested that its IT consultant evaluate these irregularities and signs of unauthorized access to the network were identified. Thereafter, the consultant immediately terminated the unauthorized access and confirmed that the network was secure. While the nature of the intrusion did not suggest that any specific private information was accessed, in an abundance of caution, HC Financial undertook further investigative efforts to identify any specific individuals whose personal information may have been compromised.

What Information Was Involved?

The forensic investigation was inconclusive as to the cause or origin of the system compromise, nor was there evidence of specific data acquisition within the mailbox. As a result, and in continuing to exhaust investigative efforts, a full and time-consuming analysis of the impacted mailbox was performed. Specifically, the investigation identified the personal information of individuals within this mailbox, including information such as social security numbers, tax identification numbers, passport numbers, and drivers' license numbers. Again, the information was available and it cannot be ruled out that it was not acquired, but there is no evidence of acquisition either. HC Financial does not have any reason to believe that this incident will result in harm to the individuals whose personal information may have been acquired or accessed as a result of this incident.

What We Are Doing

HC Financial is continuing to work closely with leading security experts to identify and implement measures to further strengthen the security of its system to help prevent this from happening in the future.

Out of an abundance of caution, we are offering you a free two-year membership to TransUnion *my*TrueIdentity 3B credit monitoring service. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. This product also includes various features such as up to $1,000,000 in identity theft insurance with no deductible, subject to policy limitations and exclusions. TransUnion *my*TrueIdentity is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft protection and TransUnion *my*TrueIdentity, including instructions on how to activate your complimentary two-year membership, please see the additional information attached to this letter. ***To take advantage of this offer, you must enroll by <<Enrollment Date>>.***

What You Can Do

We remind you to remain vigilant for incidents of fraud or identity theft by reviewing account statements and credit reports for unauthorized activity. Residents of the United States are entitled to one free credit report annually from each of the three major credit reporting agencies. To order your free credit reports, visit www.annualcreditreport.com or call toll-free (877) 322-8228. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission.

You may want to consider placing a fraud alert on your credit report. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud – an initial alert and an extended alert. You may ask that an initial alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. A fraud alert does not impact your ability to get a loan or credit, but rather alerts a business that your personal information may have been compromised and requires the business to verify your identity before issuing you credit. Although this may cause some delay if you are applying for credit, it may protect against someone else obtaining credit in your name. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies. The agency that you contacted must notify the other two agencies.

Additionally, you have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit. There is no fee to place or lift a security freeze. However, unlike a fraud alert, you must separately place a security freeze on your credit file at each of the three national credit reporting agencies.

Below are the toll-free numbers and addresses for the three largest credit reporting agencies:

Equifax
P.O. Box 74021
Atlanta, GA 30374
1-800-685-1111
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Other Important Information

Below is the toll-free number, address and website address for the Federal Trade Commission, which you may contact to obtain further information on how to protect yourself from identity theft and how to repair identity theft:

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

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont and North Carolina: 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 law 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 using the contact information listed above.

For residents of Iowa: State law advises you to report any suspected identity theft to law enforcement or 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 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

Office of the Illinois Attorney General
Identity Theft Hotline
100 W Randolph St, Fl. 12
Chicago, IL 60601
1-866-999-5630
www.illinoisattorneygeneral.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

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.

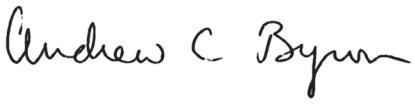
For residents of Connecticut, Massachusetts, Rhode Island and West Virginia: You also have the right to place a security freeze on your credit report by contacting any of the credit bureaus listed above.

For More Information

HC Financial values your business and understands the importance of protecting your personal information, and deeply regrets any concern this may have caused to you. Should you have any questions, please do not hesitate to contact us.

HC Financial Advisors, Inc.
3685 Mt. Diablo Blvd., Suite 200
Lafayette, California 94549-3736
Ph: (925) 299-1800
Fax: (925) 299-1812
info@hcfinancial.com
www.hcfinanical.com

Sincerely,



Andy Byron
Senior Financial Advisor and Principal

Karla McAvoy
Senior Financial Advisor and Principal

Steve Biggs
Chief Investment Officer and Principal

TransUnion

Activation Code: <<Activation Code>>

Complimentary Two-Year *my*TrueIdentity 3B Credit Monitoring Service

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online, three-bureau credit monitoring service (*my*TrueIdentity) for two years provided by TransUnion Interactive, a subsidiary of TransUnion,® one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online only

- To enroll in this service, go to the *my*TrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code **<<Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.

You can sign up for the online or offline credit monitoring service anytime between now and **<<Enrollment Deadline>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain two years of unlimited access to your TransUnion credit report and credit score.
- The daily three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion,® Experian,® and Equifax,® including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)