WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

August 16, 2018

Kevin M. Scott
312.821.6131 (direct)
Kevin.Scott@wilsonelser.com

Attorney General Joseph A. Foster
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Re: Data Security Incident

Dear Attorney General Foster:

We represent Chapman & Chapman, Inc. ("Chapman"), located in Twinsburg, Ohio, with respect to a potential data security incident described in more detail below. Chapman takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future.

1. Nature of the security incident.

On March 7, 2018, Chapman found a compromise to an employee's email account. As a result of that compromise, Chapman quickly took action and notified its Information Technology vendor of the incident, who prevented any further unauthorized access. Chapman also retained a computer forensic company and conducted a detailed forensic investigation. On June 19, 2018, it was discovered that individuals' personal information, including their name and date of birth as well as one or more of the following may have been accessed; Social Security number, insurance policy number, insurance payments (and to whom), Medicare or Medicaid number, and limited health information (medical facility, care provider, medical treatment provided, description of ailment/condition). No personal banking or credit card financial transaction or payment information was involved in this incident.

2. Number of New Hampshire residents affected.

One (1) New Hampshire resident may have been potentially affected by this incident. A notification letter to this individual was mailed on August 16, 2018, by first class mail. A sample copy of the notification letter is included with this letter.

3. Steps taken.

Chapman has taken steps to prevent a similar event from occurring in the future, and to protect the privacy and security of potentially impacted individuals' information. This includes, updating its retention rules to ensure that emails are not kept any longer than necessary, as well as training its staff to remove any unnecessary personal information that may have been provided to Chapman. Additionally, Chapman

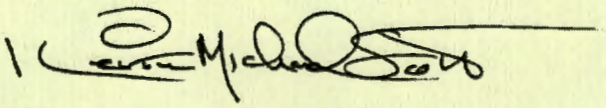
has enabled dual-factor authentication and implemented a 90-day forced password change policy. Notice is also being provided to the credit reporting agencies.

4. Contact information.

Chapman remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Kevin.Scott@wilsonelser.com or (312) 821-6131.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Kevin M. Scott

Enclosure.

August 16, 2018

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Suffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Dear <<MemberFirstName>> <<MemberLastName>>,

We are writing to inform you of a data security incident at Chapman & Chapman, Inc. that may have resulted in the disclosure of your personal information, including health information. We take the security of your information very seriously, and sincerely apologize for any inconvenience this incident may cause. This letter contains information about steps you can take to protect yourself, and resources we are making available to you.

We provide employee benefits consulting services for your employee group/health benefits plan or a plan for which you may be a beneficiary as a dependent. This notice is provided on Chapman & Chapman's and your health plan's or other employee benefit provider's behalf. On March 7, 2018, we found a compromise to a Chapman & Chapman employee's email account. As a result of that compromise, we quickly took action and notified our Information Technology vendor of the incident, who prevented any further unauthorized access. We also retained a computer forensic company and conducted a detailed forensic investigation. On June 19, 2018, it was discovered that your personal information, including your name and date of birth as well as one or more of the following may have been accessed; Social Security number, insurance policy number, insurance payments (and to whom), Medicare or Medicaid number, and limited health information (medical facility, care provider, medical treatment provided, description of ailment/condition). No personal banking or credit card financial transaction or payment information was involved in this incident.

Although we are unaware of any misuse of your or anyone's information, to help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **my.idmonitoringservice.com** to activate and take advantage of your identity monitoring services.
You have until November 24, 2018 to activate your identity monitoring services.
Membership Number: **<<Member ID>>**

To receive credit services by mail instead of online, please call 1-866-442-5364. Additional information describing your services is included with this letter.

We take the security of all information in our control very seriously, and have taken steps to prevent a similar event from occurring in the future. This includes updating our retention rules to ensure that emails are not kept any longer than necessary, as well as training our staff to remove any unnecessary personal information that may have been provided to us. Additionally, we have enabled dual-factor authentication and implemented a 90-day forced password change policy.

Please know that the protection and security of your personal information is of our utmost priority, and we sincerely regret any concern or inconvenience that this matter may cause you. If you have any questions, please do not hesitate to call 1-866-442-5364, Monday through Friday, 9:00 a.m. to 6:00 p.m. Eastern Time.

Sincerely,

Mindy Rogge
Vice President, Finance and Administration

Kroll.

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

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

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud 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.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll 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.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Additional Important Information

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 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 nationwide three 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 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, and North Carolina:

You can obtain information from the Maryland and North Carolina Offices of the Attorneys 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

For residents of Massachusetts:

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 all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus 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 credit bureaus is below:

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, or 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, 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. The consumer reporting agency may charge a small fee to place, life, or remove a freeze, but is free if you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency. You may obtain a security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
www.freeze.equifax.com
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

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