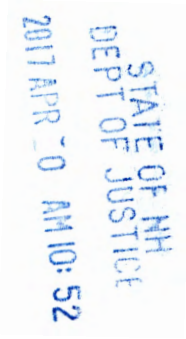
MELANIE MARIE WITTE
415.477.5731 telephone
melanie.witte@troutmansanders.com

TROUTMAN SANDERS

TROUTMAN SANDERS LLP
Attorneys at Law
580 California Street, Suite 1100
San Francisco, CA 94104
415.477.5700 telephone
troutmansanders.com

April 7, 2017



OVERNIGHT

Attorney General Joseph Foster
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Incident

Dear Attorney General Joseph Foster:

Pursuant to N.H. Rev. Stat. Ann. section 359-C:20, and on behalf of my client Campbell Taylor & Company, this incident was initially reported to you on March 18, 2017, as four (4) New Hampshire residents were determined to have been potentially affected. Investigation has completed and one (1) additional New Hampshire resident was indentified to be potentially affected in this matter. A notification letter to the additional potentially affected resident will be mailed on Friday, April 7, 2017.

NATURE OF THE UNAUTHORIZED ACCESS

After noticing some unusual activity on their network including a possible ransomware attempt, on February 13, 2017, Campbell Taylor & Company hired a specialized forensic IT firm to investigate. On February 22, 2017, the specialized forensic IT firm determined that there was unauthorized access to Campbell Taylor & Company's main network drive from a foreign IP address between January 27, 2017 and February 2, 2017, however the firm cannot determine which files were accessed. Accordingly, Campbell Taylor & Company is notifying everyone whose information was on their system out of an abundance of caution.

As an employee participant of a retirement or other benefit plan Campbell Taylor & Company performed work for, the information on their system may have included residents': first and last name, date of birth, social security number, and salary information.

NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

In total, 5 New Hampshire residents were identified as potentially affected. On March 21, 2017, 4 New Hampshire residents were mailed a notification letter; and on April 7, 2017, an additional resident was mailed notification letter. Please see enclosed for a form version of the notice.

STEPS WE HAVE TAKEN RELATING TO THE INCIDENT

In addition to the steps outlined above, Campbell Taylor & Company notified the FBI, the IRS, the FTB, all three credit bureaus, and the applicable state agencies of this incident. Further, they are reviewing office policies and procedures to ensure all security measures are taken to avoid such an incident from occurring again. In this endeavor, they hired IT specialists to determine what happened and confirm the security of their network. Lastly, Campbell Taylor & Company is providing credit monitoring for one year through AllClear ID to all potentially affected individuals, and will work with law enforcement in their investigation of the criminals.

OTHER NOTIFICATION AND CONTACT INFORMATION

A formal notification letter to the additional potentially impacted individual is being mailed Friday, April 7, 2017, the applicable state Attorney General offices and consumer affairs agencies have been notified, and Campbell Taylor & Company will assist law enforcement in the identification of the intruder in any way they can.

For any further information, please contact Melanie Witte at (415) 477-5731, melanie.witte@troutmansanders.com, Troutman Sanders, 580 California Street, Suite 1100, San Francisco, CA 94104.

Sincerely,

Melanie M. Witte

Enclosure

letterhead

[date]

[client name]
[street]
[city]

NOTICE OF DATA BREACH

Dear [CLIENT NAME]:

We are writing to provide you with information about a data incident involving Campbell Taylor & Company. You are receiving this letter because you have participated in an employee retirement or other benefit plan we have performed work for.

What Happened?

After noticing some unusual activity on our network including a possible ransomware attempt, on February 13, 2017, we hired a specialized forensic IT firm to investigate. On February 22, 2017, the specialized forensic IT firm determined that there was unauthorized access to our main network drive from a foreign IP address between January 27, 2017 and February 2, 2017, however the firm cannot determine which files were accessed. Accordingly, we are notifying everyone whose information was on our system out of an abundance of caution.

What Information Was Involved?

As an employee participant of a retirement or other benefit plan, the information on our system may have included your: first and last name, date of birth, social security number, and salary information.

What We Are Doing.

In addition to the steps outlined above, we notified the FBI, the IRS, the FTB, all three credit bureaus, and the applicable state agencies of this incident. Further, we are reviewing office policies and procedures to ensure all security measures are taken to avoid such an incident from occurring again. In this endeavor, we hired IT specialists to determine what happened and confirm the security of our network. Lastly, we are working with law enforcement in their investigation of the criminals.

What You Can Do.

Given the nature of the information potentially exposed, we strongly recommend that you monitor your accounts. Further, we strongly recommend that you contact the three credit bureaus and place a fraud alert on your accounts. Their contact information is:

Equifax	Experian	TransUnion
P.O. Box 740241	P.O. Box 2104	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
1-888-766-0008	1-888-397-3742	1-800-680-7289

You are also entitled to a free credit report every year from each of these agencies at: www.annualcreditreport.com

Next Step of Identity Protection.

As an added precaution, we have also arranged to provide you with 12 months of complimentary credit monitoring. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call **1-855-861-4034** and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. To use 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 **1-855-861-4034** using the following redemption code: {RedemptionCode}.

For More Information.

Protecting your information is incredibly important to us, as is addressing this incident with the information and assistance you may need. If you have any questions or concerns, please call AllClear ID toll free at 1-855-861-4034, or contact us directly at 916-929-3680 or 3741 Douglas Blvd, Suite 350, Roseville, CA 95661.

Very truly yours,

Campbell Taylor & Company

Further Information about Identity Theft Protection

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding 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 Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

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

For residents of Massachusetts: You also have the right to obtain a police report.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division
9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

For residents of Rhode Island: You may contact the Attorney General's office at, http://www.riag.ri.gov/ or (401) 274-4400

Fraud Alerts: There are also two types of fraud alerts that 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 fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. 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 calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax:	1-888-766-0008, www.equifax.com
Experian:	1-888-397-3742, www.experian.com
TransUnion:	1-800-680-7289, fraud.transunion.com

Credit Freezes (for Non-Massachusetts Residents): You may have the right to put a credit freeze, also known as a security freeze, on your credit file, 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 credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax:	P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian:	P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC:	P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

AllClear Identity Repair Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- 12 months of coverage with no enrollment required.
- No cost to you — ever. AllClear Identity Repair is paid for by the participating Company.

Services Provided
If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Identity Repair is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period
Service is automatically available to you with no enrollment required for 12 months from the date of the breach incident notification you received from Company (the "Coverage Period"). Fraud Events (each, an "Event") that were discovered prior to your Coverage Period are not covered by AllClear Identity Repair services.

Eligibility Requirements
To be eligible for Services under AllClear Identity Repair coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim
If you become a victim of fraud covered by the AllClear Identity Repair services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period;
- Provide proof of eligibility for AllClear Identity Repair by providing the redemption code on the notification letter you received from the sponsor Company;
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require; and
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

Coverage under AllClear Identity Repair Does Not Apply to the Following:
Any expense, damage or loss:

- Due to
  - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge, or
  - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation");
- Incurred by you from an Event that did not occur during your coverage period; or
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Identity Repair coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity.
- AllClear ID is not an insurance company, and AllClear Identity Repair is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur.
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud.
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of AllClear Identity Repair coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy
If for any reason you wish to have your information removed from the eligibility database for AllClear Identity Repair, please contact AllClear ID:

E-mail	Mail	Phone
support@allclearid.com	AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	1.855.434.8077