NORTON ROSE FULBRIGHT

Norton Rose Fulbright US LLP
Tabor Center
1200 17th Street, Suite 1000
Denver, Colorado 80202-5835
United States

Direct line +1 303 801 2758
kris.kleiner@nortonrosefulbright.com

Tel +1 303 801 2700
Fax +1 303 801 2777
nortonrosefulbright.com

June 2, 2016

By Certified Mail
Return Receipt Requested

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301

Re: Legal Notice of Information Security Incident

Dear Sirs or Madams:

I write on behalf of my client, Cohen & Grieb, P.A. ("Cohen & Grieb"), to inform you of a potential security incident that may have affected the personal information of two New Hampshire residents. Cohen & Grieb is notifying affected individuals and outlining some steps they may take to help protect themselves.

Cohen & Grieb recently learned that an unauthorized was able to gain access to its network through an account set up by an outside IT provider. Based on the information currently available, it appears that the unauthorized individual may have accessed certain client files while on the network between March 27, 2016 and April 4, 2016, when our IT provider disabled access for the affected account. The information contained in client files includes name, address, date of birth, phone number, driver's license number, Social Security number and financial account information. Cohen & Grieb previously provided notice to individuals that it identified as potentially impacted by this incident, however Cohen & Grieb's ongoing forensic investigation has identified additional individuals that may have been affected by this incident, including the two New Hampshire residents outlined above, on May 12.

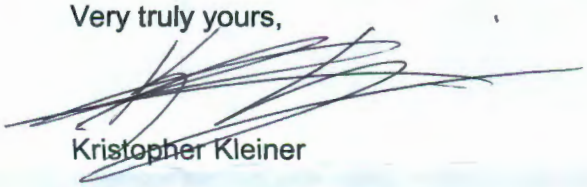
Cohen & Grieb takes the privacy of personal information very seriously, and deeply regrets that this incident occurred. Cohen & Grieb took steps to address and contain this incident promptly after it was discovered. Cohen & Grieb engaged an outside forensic expert to assist in investigating and remediating the situation. Cohen & Grieb has worked with the IT service provider and forensic firm to reconfigured various components of its systems to prevent unauthorized access and implement additional layers of protection to enhance the security of its systems. In addition, Cohen & Grieb has contacted law enforcement and will continue to cooperate in their investigation of this incident.

NORTON ROSE FULBRIGHT

Affected individuals are being notified via a written letter, which will begin mailing on or about June 7, 2016. A form copy of the notice being sent to the affected New Hampshire residents is included for your reference.

If you have any questions or need further information regarding this incident, please contact me at (303) 801-2758 or kris.kleiner@nortonrosefulbright.com.

Very truly yours,



Kristopher Kleiner

KCK
Enclosure

Cohen & Grieb, P.A.

Certified Public Accountants

500 North Westshore Boulevard • Suite 700 • Tampa, Florida 33609 • Tel: (813) 739-7200 • Fax: (813) 282-7225

Shareholders:

Donna Baptiste, CPA
Robert Cohen, CPA
Marc E. Goldstein, CPA
Robert V. Grieb, CPA
Brandy S. Guida, CPA
Jason Hamblin, CPA

DATE

[ADDRESS]

Dear [NAME],

Notice of Data Breach

Cohen & Grieb, P.A. recently learned of a potential security incident involving certain personal information of firm clients. We value our client relationships and your privacy, and we are providing this notice as a precaution to inform you of this incident and to call your attention to steps you can take to help protect yourself. We sincerely regret any frustration or concern this may cause you.

What Happened

On April 4, 2016, we learned that an unauthorized individual was able to gain access to our network through an account set up by our outside IT provider. We selected this company because they are well-regarded as one of the top local IT service providers. It appears that the unauthorized individual may have accessed certain client files while on our network between March 27, 2016 and April 4, 2016, when our IT provider disabled access for the affected account. We initially provided notice of this incident to certain of our clients who could have been affected by this incident. However, as part of our ongoing investigation of this incident, we were informed on May 12, 2016, that other Cohen & Grieb clients may also have been affected.

What Information Was Involved

It is possible that the incident may have affected certain personal information contained in your tax files, including name, address, date of birth, phone number, driver's license number, Social Security number and financial account information.

What We Are Doing

The security of our clients' personal information is of utmost importance to us. Accordingly, in conjunction with our IT service provider, immediate steps were taken to address and contain this incident upon discovery, including engaging outside forensic experts to assist us in investigating and remediating the situation. We have reconfigured various components of our systems to prevent unauthorized access and implemented additional layers of protection to enhance the security of our systems. While we are continuing to review and enhance our security measures, we believe the incident has now been contained. We have also contacted federal law enforcement and the Internal Revenue Service and we will continue to cooperate with their investigation of this incident.

What You Can Do

We want to make you aware of steps you can take to guard against fraud or identity theft. We recommend that you carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. If you find any suspicious activity on your credit reports, call your local police or sheriff's office, and file a police report for identity theft and get a copy of it. You may need to give copies of the police report to creditors to clear up your records. We also recommend that you review credit and debit card account statements as soon as possible in order to determine if there are any discrepancies or unusual activity listed. We urge you to remain vigilant and continue to monitor statements for unusual activity going forward. If you see anything you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should immediately notify the issuer of the credit or debit card. Finally, please review the "Information about Identity Theft Protection" reference guide, included here, which describes additional

steps that you may take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on placing a fraud alert or a security freeze on your credit file.

The IRS has created a Form 14039 "Identity Theft Affidavit" that helps prevent someone from filing a fraudulent tax return in your name. We are happy to prepare a Form 14039 on your behalf for no charge at your request, so please let us know if you would like us to do so. For additional information from the IRS about identity theft, please visit https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft or call 800-908-4490. There may be similar resources available at the state level, so we recommend that you contact your state department of revenue directly for more information.

In addition, to help protect your identity, we are offering twelve months of complimentary identity protection services from a leading identity monitoring services company. These services help detect possible misuse of your personal information and provide you with superior identity protection support focused on immediate identification and resolution of identity theft. For more information about these services and instructions on completing the enrollment process, please refer to the information in the "Information about Identity Theft Protection" reference guide included here.

For More Information

Please contact us for more information about this incident, or if you have additional questions or concerns.

Again, we sincerely regret any inconvenience or concern caused by this incident.

Very truly yours,

Cohen & Grieb, P.A.

Information about Identity Theft Protection

To help protect against identity theft, we are offering a complimentary twelve month membership in Experian's® ProtectMyID® service. This service helps detect possible misuse of personal information and provides superior identity protection support focused on immediate identification and resolution of identity theft. To enroll, visit **www.protectmyid.com/redeem** by **August 31, 2016** and use the following activation code: **[ACTIVATION CODE]**. You may also enroll over the phone by calling **877-371-7902** between the hours of 9:00 AM and 9:00 PM (Eastern Time), Monday through Friday and 11:00 AM and 8:00 PM Saturday (excluding holidays). Please provide the following engagement number as proof of eligibility: **PC101853**.

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the bottom of this page.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should 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 and protection against 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 North Carolina: You may also obtain information about preventing and avoiding identity theft from 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

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 contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.*

Credit Freezes: 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.

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

Equifax (www.equifax.com)
P.O. Box 740241
Atlanta, GA 30374
800-685-1111

Fraud Alerts: P.O. Box 740256, Atlanta, GA 30374
Credit Freezes: P.O. Box 105788, Atlanta, GA 30348

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

Fraud Alerts and Security Freezes:
P.O. Box 9554, Allen, TX 75013

TransUnion (www.transunion.com)
P.O. Box 1000
Chester, PA 19016
800-888-4213

Fraud Alerts and Security Freezes:
P.O. Box 2000, Chester, PA 19022
888-909-8872