



Lindsay B. Nickle
2100 Ross Avenue, Suite 2000
Dallas, Texas 75201
Lindsay.Nickle@lewisbrisbois.com
Direct: 214.722.7141

May 21, 2020

VIA E-MAIL

Gordon MacDonald, Attorney General
Consumer Protection and Antitrust Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
Email: DOJ-CPB@doj.nh.gov

Re: Notice of Data Security Incident

Dear Attorney General MacDonald:

We represent Capital Accounting & Tax d/b/a Capital Tax Service, located in Kent, Washington regarding a recent data security incident described in greater detail below. Capital Tax Service takes the protection of sensitive information very seriously and is taking steps to prevent similar incidents from occurring in the future.

1. Nature of the security incident.

On February 24, 2020, Capital Tax Service learned that fraudulent tax returns had been filed on behalf of clients using information from 2018 tax returns. As soon as this was discovered, Capital Tax Service engaged a computer forensic investigator to review the company's computer network and conduct an investigation. In addition, Capital Tax Service reached out to the IRS to identify and protect individuals whose personal information may have been involved. While the forensic investigation was inconclusive, Capital Tax Service has taken steps to harden its network and ensure the security of information it collects and stores. Based on the information learned in the investigation, the potentially impacted customer information includes names, addresses, dates of birth, Social Security numbers, tax forms, and bank routing and account numbers.

2. Number of New Hampshire residents affected.

Capital Tax Service notified one (1) New Hampshire resident via first class U.S. mail on May 21, 2020. A sample copy of the notification letter sent to the affected individuals is included with this correspondence.

3. Steps taken related to the incident.

Capital Tax Service has taken steps in response to this situation to prevent a similar occurrence from happening in the future. Those steps include scanning all systems for malware, closure of all unused ports, resetting of all passwords, and updating of routers and firewalls. In addition, Capital Tax Service is continuing to collaborate with IRS fraud detection and prevention efforts.

Capital Tax Service is also offering twelve (12) months of complimentary identity theft protection services to all affected persons through ID Experts. ID Experts' product includes credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services.

4. Contact Information.

Capital Tax Service remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact me at (214) 722-7141 or by e-mail at lindsay.nickle@lewisbrisbois.com.

Sincerely,



Lindsay B. Nickle of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl.: Consumer Notification Letter

4828-3038-4828.1



CAPITAL TAX SERVICE
 TAX PREPARATION & DEBT RESOLUTION
 www.capitaltaxservice.net

C/O ID Experts
 10300 SW Greenburg Rd. Suite 570
 Portland, OR 97223

To Enroll, Please Call:
 1-800-939-4170
 Or Visit:
<https://app.myidcare.com/account-creation/protect>
 Enrollment Code: <<XXXXXXXXXX>>

<<First Name>> <<Last Name>>
 <<Address1>> <<Address2>>
 <<City>>, <<State>> <<Zip>>

May 21, 2020

Re: Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>,

We are writing to inform you of a potential data security incident that may have affected your personal information. Capital Tax Service takes the privacy and security of your personal information very seriously. We are sending you this letter to notify you about this incident, offer you credit and identity monitoring services, and inform you about steps you can take to protect your personal information.

What Happened? At the end of February 2020, we noticed a higher than usual reject rate for tax returns filed by Capital Tax Service. We then discovered that many of these tax filings were rejected because fraudulent tax returns had already been filed in clients' names with contents mirroring those found in clients' 2018 returns. We immediately began investigating the situation and reached out to the IRS. We also hired computer security experts to assist us. While it is not precisely known how or when your tax information may have been compromised, based on what we have learned from the IRS, it is possible someone without authorization may have accessed your tax information and may have filed a tax return in your name without your authorization.

What Information Was Involved? The following information may have been accessed: your name, address, date of birth, Social Security number, tax forms, and bank routing and account numbers.

What Are We Doing? As soon as we discovered the incident, we took the steps referenced above. We have also enhanced the security of our systems. We are continuing to work with the IRS to try and prevent fraudulent filings and to hold the perpetrators accountable. In addition, we are offering credit and identity monitoring services for 12 months at no cost to you and providing you additional information about steps you can take to protect your personal information.

What You Can Do. You can follow the recommendations on the following page to protect your personal information. Also, if you haven't already done so, we encourage you to complete IRS Form 14039, Identity Theft Affidavit which you can obtain at <http://www.irs.gov/pub/irs-pdf/f14039.pdf>, and then mail or fax it to the IRS according to the instructions on the form. Please contact us should you need assistance filing the Form 14039. If you have other identity theft/tax related issues, contact the IRS Identity Protection Specialized Unit at 1-800-908-4490.

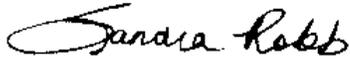
In addition, we are offering identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised. 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. You can enroll in free MyIDCare services by calling 1-800-939-4170 or going to

<https://app.myidcare.com/account-creation/protect> and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is August 21, 2020.

We encourage you to take full advantage of this service offering. MyIDCare representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information. Please follow the directions in this letter to enroll for services. You will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter. Please call 1-800-939-4170 or go to <https://app.myidcare.com/account-creation/protect> for assistance or for any additional questions you may have.

Sincerely,

A handwritten signature in black ink that reads "Sandra Robb". The signature is written in a cursive style with a large, flowing "S" at the beginning.

Sandra M Robb
Capital Tax Service

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. 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 also should 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 (FTC).

In the Event of Fraudulent Unemployment Filings: Please be aware that information commonly found in tax filings is often sufficient to enable fraudulent filings for unemployment benefits. If you believe this has happened to you, then please contact the state department in your home state responsible for administering unemployment benefits. This department is in the best position to assist you. Washington State residents: contact the Employment Security Department at: www.esd.wa.gov, P.O. Box 9046, Olympia, WA 98507, ph.: 1-800-246-9763, email: ESDGPInternalFraud@ESD.WA.GOV.

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

| | | | |
|--|--|--|--|
| TransUnion | Experian | Equifax | Free Annual Report |
| P.O. Box 1000 | P.O. Box 9532 | P.O. Box 105851 | P.O. Box 105281 |
| Chester, PA19016 | Allen, TX 75013 | Atlanta, GA 30348 | Atlanta, GA 30348 |
| 1-800-909-8872 | 1-888-397-3742 | 1-800-685-1111 | 1-877-322-8228 |
| www.transunion.com | www.experian.com | www.equifax.com | www.annualcreditreport.com |

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Contact information for the FTC is:

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
www.consumer.ftc.gov
www.ftc.gov/idtheft
1-877-438-4338

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information, as well as others. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf