

David B. Cheatham, CPA
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>>

Notice of Data Breach

Dear <<Name 1>>:

Thank you for allowing David B. Cheatham, CPA, to serve your income tax needs. We take the issue of privacy seriously and, as part of that commitment, we are sending you this letter to make you aware of a recent data security incident that may have affected your personal information. Please read this letter carefully.

What Happened

On December 8, 2018, a computer hard drive containing some of our clients' information was stolen from our office. While the hard drive was password-protected, it is possible that the person responsible for the theft may have been able to access the data on the hard drive if he or she was able to circumvent the password protection.

What Information Was Involved

We cannot confirm whether the person who stole the hard drive was able to access any data on it or which specific data, if any, he or she may have accessed. However, our investigation of the incident has confirmed that the hard drive did contain some of our clients' information, including tax documents containing your name, address, date of birth, and Social Security Number. It is thus possible that there has been unauthorized access to this information.

What We Are Doing

Please know that we take the protection of our clients' personal information seriously and we are taking steps to continue investigating this incident, help mitigate the potential for harm, and prevent future incidents from happening. At this time, we have not found the person behind the theft or determined his or her motives, but we have notified law enforcement and the IRS and will continue cooperating with their investigations. Out of an abundance of caution, we also have changed all passwords used to access our computer system, and we are reviewing our policies and procedures to identify any additional ways to further strengthen the confidentiality and security of our clients' information.

What You Can Do

In light of this incident, we recommend that you remain vigilant by reviewing and monitoring your account statements and credit reports. If you find any errors or unauthorized activity, you should contact your financial institution or call the number on the back of your payment card. You also may file a report with law enforcement, your state attorney general, and/or the Federal Trade Commission. In addition, please refer to the enclosed documentation which contains additional steps you may take to protect your information from misuse, including some information that may be specific to your state of residence.

As an added precaution to help protect your information from potential misuse, we are offering complimentary credit monitoring and identity theft restoration services through *myTrueIdentity* provided by TransUnion Interactive, a subsidiary of TransUnion®, at no cost to you. *myTrueIdentity* services include 12 months of credit monitoring and alerts, a \$1,000,000 insurance reimbursement policy, educational materials, and ID theft recovery services. *myTrueIdentity* will help reduce the risk of identity theft and also help you resolve issues in the event your identity is compromised.

To enroll in *myTrueIdentity* online or by telephone, please refer to the enclosed documentation containing your enrollment instructions and your personal activation codes. Please note that you must complete enrollment by <<**Enrollment Deadline**>>. In addition, please carefully review the information in the enclosed documentation about further steps you may take to help protect your personal information from misuse.

For More Information

We very sorry for any concern or inconvenience this incident has caused or may cause you. If you have any other questions or concerns that you would like to discuss, you may contact us through our dedicated hotline at 877-431-9931 between 6:00 a.m. and 6:00 p.m. Pacific Time, Monday through Friday.

Sincerely,

David B. Cheatham, CPA

myTrueIdentity Enrollment Instructions and Recommended Steps to Help Protect Your Information

- 1. Enroll in myTrueIdentity online or by telephone.** You may enroll in the *myTrueIdentity* services on the website www.mytrueidentity.com. In the space where it states, "Enter Activation Code", enter the following 12-letter Activation Code <<**Unique 12-letter Activation Code**>> and follow the steps to receive your credit monitoring service online within minutes. If you do not have internet access or wish to enroll in an offline, paper-based credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at (855) 288-5422. When prompted, enter the following 6-digit telephone passcode <<**Static 6-digit Telephone Passcode**>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

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.

- 2. Review personal account statements and credit reports.** We recommend that you remain vigilant by reviewing personal account statements and monitoring credit reports to detect any errors or unauthorized activity. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call (877) 322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months. If you discover any suspicious items and have enrolled in *myTrueIdentity*, notify them immediately. Otherwise, you should report any incorrect information on your report to the credit reporting agency.
- 3. Report suspected fraud.** You have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You should report suspected incidents of identity theft to local law enforcement, your state's Attorney General, and/or the Federal Trade Commission.
- 4. Place Fraud Alerts** with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert 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 bureaus is as follows:

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348
www.alerts.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022
www.transunion.com

It is only necessary to contact one of these bureaus and use only one of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review.

- 5. Security Freeze.** By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above in writing to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. The cost of placing the freeze varies by the state you live in and for each credit reporting bureau. The Credit Bureau may charge a fee of up to \$5.00 to place a freeze, lift, or remove a freeze. However, if you are a victim of identity theft and have filed a report with your local law enforcement agency or submitted an ID Theft Complaint Form with the Federal Trade Commission, there may be no charge to place the freeze.

6. **You can obtain additional information** about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

- **California Residents:** Visit the California Office of Privacy Protection, www.privacy.ca.gov, for additional information on protection against identity theft.
- **Iowa Residents:** Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, (515) 281-5164.
- **Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, (502) 696-5300.
- **Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, (888) 743-0023.
- **North Carolina Residents:** Office of the Attorney General of North Carolina, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.com, (919) 716-6400.
- **Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us, (877) 877-9392.
- **Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, (401) 274-4400.
- **All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.ftc.gov, 1-877-IDTHEFT (438-4338).

Summary of Rights Under the Fair Credit Reporting Act. The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. You have certain rights under the FCRA, including: (1) You must be told if information in your file has been used against you; (2) You have the right to know what is in your file (you “file disclosure”); (3) You have the right to ask for a credit score; (4) You have the right to dispute incomplete or inaccurate information; (5) Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (6) Consumer reporting agencies may not report outdated negative information; (7) Access to your file is limited to people with a valid need; (8) You must give your consent for reports to be provided to employers; (9) You may limit “prescreened” offers of credit and insurance you get based on information in your credit report; (10) You may seek damages from violators; and (11) identity theft victims and active duty military personnel have additional rights. For more information, visit www.ftc.gov/credit. States may enforce the FCRA, and many states have their own consumer reporting laws. In some cases, you may have more rights under state law. For more information, contact your state or local consumer protection agency or your state Attorney General.