



133 Old Wards Ferry Road, Suite J • Sonoma, CA 95370
Tel: 209.536.1218 - Fax: 209.536.1259 – www.WEcpas4u.com



03073
TO THE ESTATE OF JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

September 13, 2016

NOTICE OF DATA BREACH

To the Estate of John Sample,

We are writing to provide you with notification regarding a data breach involving our office desktop network computers, in which your personal information may have been compromised. You are receiving this letter as a beneficiary of a trust for which we provide(d) tax services.

What Happened, Including an IRS Newswire e-mail Update:

On August 15, we discovered a data security incident involving our firm and some of our clients whose 2015 tax returns were on Extension. After thorough investigation, we have discovered that the perpetrator(s) hacked into our system, and between August 3rd and 9th 2016, fraudulently filed 45 client tax returns. Although we are unaware of any false tax return having been filed under your name or company, we are notifying you of this incident because your tax information may have been exposed.

On September 2, 2016, the IRS Newswire email stated, “The IRS is aware of approximately two dozen cases where tax professionals have been victimized in recent days.” Unfortunately, our firm was a firm victimized in these targeted attacks.

What Information Was Involved?

If you are an individual, this information may have included your name, gender, date of birth, telephone number(s), address, Social Security number, all employment (W-2) information, 1099 information, as well as direct deposit bank account information, including account number and routing information (if provided to us); further, supporting documentation including brokerage statements and other types of specific documents you may also have provided to us.

If you are an entity, this information may have included your company name, Federal Employer Identification Number, address, telephone number; employee and/or 1099-recipient information; partner, shareholder/officer or beneficiary names, addresses, Social Security numbers; and/or other information stored in our computers.

What We Have Done So Far:

- Based on the **diligent investigative work** of **both** our local IT consultant and that of an IT firm from the Bay Area:
 1. The **malware** on the impacted computers’ hard drives has been **removed**.
 2. We have made **internal software system management changes**.
 3. All network firewalls, computers and **security protections** are **confirmed to be properly functioning**.
 4. **Both IT firms** will continue working **together with us** to prevent a future data breach.



01-04-1-00

• We are working with appropriate agencies on your behalf regarding the following:

1. The IRS, FTB, FBI, FDIC and the US Secret Service have been made aware of the 45 fraudulent filings. Your return has been placed on the IRS and FTB's Fraud Alert. We are working with these agencies to assist in their investigation and interruption of intent of the cyber intruder(s).
2. The Police Report with the FBI's online Internet Crime Complaint Center (IC3) was updated August 31, 2016. A copy is available upon request.
3. All three consumer reporting agencies have been notified regarding the incident.
4. We have notified the offices of the applicable State Attorney Generals.

What You Can Do:

- Given the breadth of information exposed, we strongly recommend you are vigilant in reviewing all bank account and brokerage statements, as well as free credit reports.
- We suggest that you change the bank account numbers you provided us, and/or have a conversation with your bank regarding the monitoring to be provided by them as well as yourselves. It is also recommended that you change your passwords on all accounts, bank and brokerage.
- We also suggest you contact the FTC at 1-877-438-4338 and the Social Security Administration at 1-800-772-1213.
- You can call the three major credit agencies and place a 90-day fraud alert on your accounts. If you want to pursue that further, their contact information is:

| | | |
|---|--|--|
| Equifax P.O. Box 740241 Atlanta, GA 30374 1-800-525-6285 https://www.alerts.equifax.com/AutoFraudOnline/jsp/fraudAlert.jsp | Experian P.O. Box 2104 Allen, TX 75013 1-888-397-3742 https://www.experian.com/fraud/center.html | TransUnion P.O. Box 2000 Chester, PA 19022 1-800-680-7289 https://fraud.transunion.com/fa/fraudAlert/landingPage.jsp |
|---|--|--|

- You are also entitled to a free credit report every year from each of these three agencies at: www.annualcreditreport.com
- If you suspect identity theft, report it to law enforcement, including the FTC at <https://www.identitytheft.gov/Assistant#>

Next Step of Identity Protection:

We are providing you with one year of complimentary credit monitoring. We have already paid for both levels of protection provided by AllClear ID to protect your identity for 1 year. You only need to sign up for Level 2, AllClear Credit Monitoring; you are automatically protected under AllClear Identity Repair.

1. The AllClear Identity Repair protection services start on the date of this notice and you can use them at any time for one year from the date of this notice. The team at AllClear ID is ready and standing by if you need identity repair assistance. This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-303-6663 and a dedicated investigator will help recover financial losses, restore your credit, and make sure your identity is returned to its proper condition.
2. AllClear Credit Monitoring: To start this active relationship involved at the PRO service level, you have to enroll. Contact the company and sign up for it; you will need to provide your personal information to AllClear ID. This service offers additional layers of protection including: (1) credit monitoring and, (2) a \$1 million identity theft insurance policy. Additionally, for a child under 18 years old, AllClear ID ChildScan identifies acts of credit, criminal, medical or employment fraud against children by searching thousands of public databases for use of your child's information. You may sign up online at <https://enroll.allclearid.com/> or by phone by calling 1-855-303-6663 using the following redemption code: [REDACTED] Please note: Additional steps may be required by you in order to activate your phone (text) alerts and monitoring options.

Information about Identity Theft Protection

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 below.

Equifax: P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com
Experian: P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion: P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

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

The next 2 paragraphs are regarding incidents involving personal health information. Disregard if not applicable to your situation.

We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the web site of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

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



03-04-6

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.

Credit Freezes (for Massachusetts Residents): Massachusetts law gives you the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below:

| | |
|-----------------|--|
| 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 |

Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). The credit reporting company may charge a reasonable fee of up to \$5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company.

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 that occurred 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;
- 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
 - 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;
- 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; and
- 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 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 support@allclearid.com | Mail AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701 | Phone 1.855.434.8077 |
|---|--|--------------------------------|

