MARTIN
HUTCHISON &
HOHMAN

THOMAS W. MARTIN
RETIRED
RICHARD A. HUTCHISON
MICHELLE A. HOHMAN

**Certified Public Accountants**
2601 Harrison Avenue, Eureka, CA 95501

www.cuttaxnow.com ▪ mhh@cuttaxnow.com
(707) 445-8476 ▪ fax (707) 445-8477

# Notice of Data Breach

February 19, 2019

My Dear Tax Clients,

It is with deepest regret that I send this letter to you in order to inform you of a recent event in our firm.

## What Happened?

On Friday, February 15, 2019, while trying to resolve an email failure with our email host, Suddenlink, I was directed to a website that gave a phone number to call for immediate assistance. When I called this number, the technician stated he could certainly help. He requested access to my computer to understand the issue with the email. After I installed the software necessary to give him remote access to my computer, he pulled up some IP addresses on my computer screen and stated that this was the reason for the email failure. He then insisted that in order to fix the problem and prevent viruses from attacking, I would need to allow him to install a program on our office's network server. I told him no and that our local computer technician would be contacted to deal with this. At that point, he stated that only a Microsoft Tech such as himself would be able to do this. This was a red flag as I thought I was dealing with a Suddenlink technician. At that point, I quickly disconnected my computer from the internet and from our office network. I then uninstalled the remote access software I had just allowed him to install, and turned the computer off. This entire interaction lasted less than eight minutes.

Our local computer technician was contacted immediately. They indicated that this was a known scam and that they try to copy information that exists on the computer they are given access to and, to their knowledge, are not able to move beyond that initial local hard drive quickly, if at all.

## What Information Was Involved?

The information that was most at risk of being breached were those documents in the "My Documents" folder on my computer as well as those saved on my computer. On my desktop, I kept a folder of items that had been emailed. If I have emailed a copy of your tax returns or other document, which contains your personal data, in the recent past, your data was most at risk of being compromised. We also discovered that older years of our tax program saved on my computer were not encrypted. At this time, it is unknown what, if anything, was taken from my computer in the short amount of time that the breach occured.

## What Are We Doing?

The computer was immediately taken to our computer technician's shop for a virus check and cleaning. I learned the next morning that the computer was infected with a sophisticated virus that could not be prevented by normal virus protection software. The hard drive was then replaced in order to prevent any risk of further infection. It is still unknown if any client information on our computer network was compromised. At this time, there is no indication of further infection involving our computer network.

We are performing virus scans of all computers; upgrading virus software as needed. In addition, we are changing physical controls which include storing more, if not all, of our client data in an encrypted form. The majority of our

client data has been maintained in encrypted form for some time. However, we are working to review all of our data storage to ensure that everything possible is stored this way.

In addition, we will no longer allow an outside technician to remotely access any computer on our network. Lastly, and most importantly, we are sending out this notification as quickly as possible to all those potentially affected.

What Can You Do?

Please take a moment and assess the following link below on what you can do to protect yourself in a security breach.
https://www.privacyrights.org/how-to-deal-security-breach

In addition, due to the unknown risk of your own personal data being compromised, I suggest that you contact your credit agency and have either a freeze or fraud alert placed on your account. Both of these are free.

> What do fraud alerts and credit freezes do? With a fraud alert, businesses must try to verify your identity before extending new credit. Usually that means calling to check if you're at a particular store attempting to take out new credit. With a credit freeze, no one – including you – can access your credit report to open new accounts. You'll get a PIN number to use each time you want to freeze and unfreeze your account to apply for new credit.

The contact numbers for the Credit Agencies are;

Transunion 800-909-8872 Experian 888-397-3742 Equifax 800-685-1111

Regardless of the threat from the above security breach, placing a fraud alert or freeze on your credit helps to prevent identity theft.

For more information on how to protect yourself from Identity Thefts, we have enclosed the IRS Identity Protection Tips and here are a couple of websites you may wish to review.

https://www.experian.com/blogs/ask-experian/how-to-protect-yourself-from-identity-theft/

https://www.creditkarma.com/id-theft/i/how-to-protect-yourself-from-id-theft/

I recommend that you closely monitor your credit activity and financial accounts. Please notify me at once if there is any irregularity so that I may assist you in taking corrective action and can notify other clients of the breach.

I am so sorry this happened and for any inconvenience and anxiety this may cause you or your loved ones. I appreciate the trust you put in me and I will do everything possible to continue to warrant that trust.

Sincerely,

Richard A. Hutchison
Martin, Hutchison and Hohman, CPAs

IRS

# Identity Protection Tips

Tax-related identity theft occurs when someone uses your stolen Social Security number to file a tax return claiming a fraudulent refund. You may be unaware you are a victim until you receive an IRS notice or you file your return, but it is rejected because your SSN already has been used. It's important that you take steps to protect all of your personally identifiable information.

**Don't fall for common scams**

- An unexpected email purporting to be from the IRS is always a scam. The IRS does not initiate contact with taxpayers by email or social media to request personal or financial information. If you receive a scam email claiming to be from the IRS, forward the email to phishing@irs.gov.
- An unexpected phone call from someone claiming to be an IRS agent, either threatening you with arrest or deportation if you fail to pay immediately, is a scam. In another variation, the caller requests your financial information in order to send you a refund. Report these calls and other IRS impersonation schemes to the Treasury Inspector General for Tax Administration at 1-800-366-4484 or online at IRS Impersonation Scam Reporting.
- If you discover a website that claims to be the IRS but does not begin with 'www.irs.gov,' forward the link to phishing@irs.gov.

**Tips to protect your SSN and identifiable information**

- Keep your card and any other document that shows your Social Security number in a safe place; DO NOT routinely carry your card or other documents that display your number.
- Be careful about sharing your number, even when you are asked for it; ONLY share your SSN when absolutely necessary.
- Protect your personal financial information at home and on your computer.
- Check your credit report annually.
- Check your Social Security Administration earnings statement annually,
- Protect your personal computers by using firewalls, anti-spam/virus software, update security patches and change passwords for Internet accounts.
- Protect your personally identifiable information; keep it private. Only provide your SSN when YOU initiate the contact or you are sure who you know is asking.

**About data breaches**

Not all data breaches or computer hacks result in identity theft and not all identity theft is tax-related identity theft. It's important to know what type of personally identifiable information was stolen. For example, did a data breach compromise your credit card or did it compromise your SSN?

If you've been a victim of a data breach, keep in touch with the company to learn what it is doing to protect you. Follow the steps recommended by the Federal Trade Commission's www.identitytheft.gov site.

If your SSN was compromised, follow the steps outlined in the Taxpayer Guide to Identity Theft.