KINGSBERY CPAs
KINGSBERY • BARIS • VOGEL • NUTTALL

Notice to Kingsbery CPAs Clients Regarding the Recent Equifax Data Breach

As you know, Equifax, one of the three main credit bureaus, was recently breached. We encourage you to check your credit and read this bulletin from the IRS:

A data breach is the intentional or unintentional release or theft of secure information. It can be the improper disposal of personally identifiable information in the trash or a sophisticated cyber-attack on corporate computers by criminals. It can affect companies large or small. The one common link is the victim, the person whose identity, financial or personal information has been compromised.

Here's what you should know about data breaches:

Not every data breach results in identity theft, and not every identity theft is tax-related identity theft.

Tax-related identity theft is when someone uses your Social Security number to file a false tax return claiming a fraudulent refund. Your tax account is most at risk if the data breach involves both your SSN and financial data, such as wages. Data breaches involving just credit card numbers, health records without SSNs or even drivers' license numbers, while certainly serious, will not affect your tax account. The Internal Revenue Service is committed to working with taxpayers to ensure that all tax accounts remain secure.

The IRS stops the vast majority of fraudulent tax returns. If fraud is suspected, the IRS will contact you via mail with instructions. Or, you may attempt to file electronically and your return is rejected as a duplicate.

If you are a data breach victim, take these steps:

If possible, determine what type of Personally Identifiable Information (PII) has been lost or stolen. It is important to know what kind of information has been stolen so you can take the appropriate steps. For example, a stolen credit card number will not affect your IRS tax account.

Stay informed about the steps being taken by the company that lost your data. Some may offer special services, such as credit monitoring services, to assist victims.

Follow the Federal Trade Commission recommended steps, including:

- Notify one of the three major credit bureaus to place a free fraud alert on your credit file;
- Consider a credit freeze, which, for a fee in some states, will prevent access to your credit records;
- Close any accounts opened without your permission;
- Visit www.identitytheft.gov for additional guidance.

If you received IRS correspondence indicating you may be a victim of tax-related identity theft or your e-file tax return was rejected as a duplicate, take these additional steps with the IRS:

- Submit an IRS Form 14039, Identity Theft Affidavit
- Continue to file your tax return, even if you must do so by paper, and attach the Form 14039
- Watch for any follow-up correspondence from the IRS and respond quickly.

Who should file a Form 14039?

This form should be used if your Social Security number has been compromised and IRS has informed you that you may be a victim of identity theft tax fraud or your e-file return was rejected as a duplicate. The fillable form is available at IRS.gov. Follow the instructions exactly. You can fax or mail it or submit it with your paper tax return if you have been prevented from filing because someone else has already filed a return using your SSN. You only need to file it once.

https://www.irs.gov/identity-theft-fraud-scams/data-breach-information-for-taxpayers

Other recommendations from Kingsbery CPAs:

Check your credit reports - If you're not sure if your data was affected, consider looking through your credit reports for any suspicious activity. The US government guarantees everyone a free annual credit report from the three major bureaus – including Experian via this link:
https://www.ftc.gov/faq/consumer-protection/get-my-free-credit-report

When looking through your reports, keep an eye out for new accounts you didn't open, late payments on debts you don't recognize and any other activity that looks unfamiliar.

If you suspect someone used your identity to open credit cards, take on loans, or re-open closed accounts, contact the credit card company's fraud department immediately. You are not responsible for charges made on a fraudulent card, but you have to report the issue in a timely manner. Once you've reported the fraudulent credit, follow this guide to recovering from identity theft.

To set a fraud alert, contact just one of the credit card bureaus and ask for an initial fraud alert. Once the alert is set, it will last 90 days. After that, you'll have to renew it. Here are the appropriate phone numbers for the bureaus (remember, just call one):

- Equifax: 1-888-766-0008
- Experian: 1-888-397-3742
- TransUnion: 1-800-680-7289

Equifax Links Regarding Data Breach

Equifax has developed a Progress Updates for Consumer's page on their website.
Equifax has also developed a page with frequently asked questions.

Please feel free to contact your Kingsbery CPAs tax advisor if you need additional guidance.