October 2017 Identity Theft Client Memo

The Equifax breach: what you should know

In September, major credit reporting agency Equifax disclosed a data breach that potentially affected roughly 143 million Americans.

Are you worried about the safety of your personal information? Here's what you should know:

1. **What was exposed**
   Names, Social Security numbers (SSNs), birth dates, addresses, driver's license numbers, credit card numbers and dispute documents. Hackers accessed this data from mid-May through July 2017.

2. **How to know if your data was breached**
   Equifax is asking consumers to visit its website (www.equifaxsecurity2017.com). You can enter the last six digits of your SSN to find out if your personal info may have been impacted by the breach.

3. **How Equifax is responding**
   Equifax is offering free credit monitoring and identity theft protection to people, whether or not they were affected by the July breach.

4. **What you can do right now**
   It's daunting to think your personal data may have been hacked, but there are still steps you can take to protect it:
   - **Review your credit card and bank account activity.** Keep an eye out for any strange transactions or overspending.
   - **Put a credit freeze and/or fraud alert on your files.** A credit freeze can make it more difficult for someone to open a new account using your name. A fraud alert offers a heads up to creditors that you may be an identity theft victim.
   - **Check for accounts you don't recognize with a credit report.** New accounts opened in your name or activity you don't recognize might be a sign of identity theft.

Unfortunately, you may not find out you're a victim of identity theft for months after a breach. The best way you can protect yourself is to stay vigilant with your accounts and credit activity.

Let us know if you think you've been affected by a data breach. We can work with you to make sure your taxes are filed as soon as possible – giving an identity thief less time to file a fraudulent claim using your personal info.

Phishing and malware on the rise – Protect yourself

The IRS reported there was an approximately 400 percent increase in phishing and malware scams during the 2016 tax season. The best way you can protect yourself this tax season is to find out how identity thieves are stealing data and what you can do to combat it.

- **How phishing and malware schemes work:** Scammers will send taxpayers emails and text messages that look like they're from the IRS, tax software companies or other official groups.

  The communications will include requests for important information needed for filing. Sometimes links to impostor websites are included. They are meant to look legitimate and gather data that will later be used to file false tax returns. Malware is also used to infect computers and let thieves access your info and track what you type on your keyboard.

- **What the IRS is doing about it:** The IRS, together with tax industry leaders and tax commissioners, make up the Security Summit Group. This team is in its third year of protecting taxpayer data through new safeguards and public programs about identity theft security. There's been a 53 percent drop from 2015 to 2016 in identity theft victim reports.

- **How you can protect yourself:** Don't reply to unsolicited emails or texts claiming to be from the IRS or the Electronic Federal Tax Payment System (EFTPS) asking for sensitive info related to your taxes. Instead, report them to the IRS at phishing@irs.gov.

  The IRS will not initiate contact with you by email or text to request financial or personal info, including PIN numbers and passwords.

Give us a call today if you want to know more about how to protect your tax info from identity theft, and if you have other questions about preparing for the upcoming tax season.