SignatureEXEC

Identity Theft and the Targeting of High-Net-Worth Families

By Blake Williams, Senior Planning Associate

If you think celebrities like Tiger Woods, Will Smith, Michelle Obama and Bill Gates are immune from identity theft, think again. All of them have been victims of identity theft. In actuality, everyone is a target for identity theft, but affluent individuals and families are more likely to be targeted due to their high profile and potential for a big payout.

It's becoming common for society to readily accept that a large data breach has happened. This spring, health insurer Anthem revealed that hackers stole the Social Security numbers and personal information for nearly 80 million Americans.[1] This summer the IRS was targeted by hackers who stole sensitive personal information from over 600,000 Americans.[2] On the heels of the IRS declaration, the FBI announced it was investigating one of the largest-ever thefts of government records at the U.S. Office of Personnel Management. It's estimated that hackers accessed security clearance forms and Social Security numbers for somewhere between 4 million and 18 million current and former employees.[3] These are alarming numbers, especially when they are just for 2015! The discussion about these data breaches may fade quickly, but what won't fade is the access that thieves have to their victims' sensitive personal information.

> **"Everyone is a target for identity theft, but affluent individuals and families are more likely to be targeted due to their high profile and potential for a big payout."**

The question you are probably asking yourself is, "If these breaches are so common, how can I protect myself against identity theft when the wealthiest individuals and government entities, with vast resources at their disposal, become a victim?"

Credit Freezes

The strongest preventative measure available to deter identity theft is to freeze your credit with Experian, TransUnion and Equifax. Thieves will be unable to obtain new extensions of credit with a credit freeze in effect. If you suspect that your personal information has been compromised, we strongly suggest freezing your credit. For an in-depth review with step-by-step instructions on how to freeze your credit, please view our "Safeguarding Your Identity" blog post.

Credit Monitoring Services

While a credit freeze is a strong preventative measure, it wouldn't help with certain types of identity theft, such as tax fraud, medical fraud and even driver's license identity theft. This is where credit monitoring services can assist. The main benefit of these services is that they are designed to alert you to suspicious activity, and in the event you do become a victim of identity theft, their team of experts can help restore your identity. Many insurance companies also include identity theft restoration coverage under the homeowner's policy once a breach has occurred.

One of the fastest-growing types of identity theft is medical identity theft. Medical identity theft occurs when thieves steal an individual's personal information and use it to obtain emergency care, medical equipment, prescriptions and even surgery! Medical identity theft saw a 20 percent increase from 2012 to 2013 alone, with an average cost of $18,660 per victim.[4] There have been medical identity theft cases where health care providers refused an individual access to their own health record because it would violate the identity thief's privacy rights! In this situation, you'd have to appeal to the U.S. Department of Health and Human Services' Office for Civil Rights.[5] Medical identity theft is extremely difficult for credit monitoring services to detect due to federal health care privacy laws. However, if medical identity theft happens to you, this is the benefit of having a team of experts from a credit monitoring service facilitate the repair process.

Rather than utilize a credit monitoring service, many people choose to periodically review their credit report on their own. For a detailed review of credit monitoring services and instructions on how to check your credit report, please view our "Safeguarding Your Identity" blog post.

The IRS Tax PIN

Each spring, there is a rush of news headlines on tax-related identity theft. Tax identity theft occurs when someone uses a stolen Social Security number to file a tax return claiming a fraudulent refund. Generally, an identity thief will use a stolen Social Security number to file a false return early in the year.[6] Imagine your dismay when you file your tax return and it is rejected because someone has already filed on your behalf!

There is hope in the fight against tax identity theft! Taxpayers who filed federal returns last year from **Georgia, Florida** or the **District of Columbia** are eligible for the IRS Identity Protection PIN program. These three regions have the highest per-capita percentage of tax-

related identity theft.[7] If you've ever been a victim of tax identity theft, you are also eligible for the IRS PIN program.

Please see the attachment for instructions on how to sign up for the IRS PIN program.

Danger of Public Wi-Fi vs. Mobile Hot Spots

Have you ever logged in to a Wi-Fi network at a coffee shop or at a hotel while traveling? You may have put yourself at risk. High-net-worth insurance provider PURE recently revealed that hackers are targeting hotel Wi-Fi networks to access affluent individuals' information. Researchers discovered a vulnerability in routers belonging to eight of the world's top 10 hotel chains. At least 277 routers in 29 countries were believed to have been impacted. Of these, more than 100 were at locations in the U.S. Through the router, attackers were able to install a very sophisticated keystroke logger on guests' computers.[8] We recommend using the hot spot feature on your cellphone as the networks for large cellular carriers are seen to be more secure than public Wi-Fi and they encrypt your data.

Other common identity theft tactics include Wi-Fi spoofing and phishing attacks. Wi-Fi spoofing attacks occur when thieves create a Wi-Fi account that has a similar name to your personal network in hopes that you'll join it. If you mistakenly do this, they have a wide-open view of what you are doing on the Internet. When Internet identity thieves impersonate an individual or business to trick you into giving out your personal information, it's known as phishing. Most of us have been recipients of attempted phishing schemes. However, "spear phishing" is much more targeted, especially for high-profile individuals. Executives with more than 2,500 employees have a 1 in 2.3 chance of becoming the target of a spear phishing attack.[9] Spear phishing occurs when thieves target a specific individual and include personal data gathered through social media in order to appear legitimate, including names of business colleagues, friends and family.

While we must be continuously vigilant in our actions on the Web, there are services that can make our lives easier while providing an additional element of security for our online login credentials. The sheer number of websites, user names, passwords and security features that we each have to remember is mind-boggling. Password managers are services that enable you to securely save all your passwords in a central location and keep them safe by using one master password. For a comprehensive review of several of the leading password manager services, please see our "Protect Yourself with a Password Manager" blog post.

Conclusion

Identity theft via the Internet is a topic that will continue to draw headlines. *Chief Executive* magazine revealed that the majority of CEO respondents view cyber security as their greatest personal risk, rating it higher on their list of concerns than natural disasters and home invasions.[10] While it seems increasingly improbable that our personal data can be sufficiently safeguarded, whether by the government or the private sector, it is ever more important that individuals be vigilant with the security of their personal information and take safeguards to ensure that criminals can't use it in the event it becomes compromised.

Sources

1. Gregory McNeal, "Health Insurer Anthem Struck by Massive Data Breach," *Forbes*, February 4, 2015, www.forbes.com/sites/gregorymcneal/2015/02/04/massive-data-breach-at-health-insurer-anthem-reveals-social-security-numbers-and-more/.

2. Lisa Rein, "IRS Says Breach of Taxpayer Data Far More Widespread Than It First Thought: 610,000 Taxpayers at Risk," *The Washington Post*, August 17, 2015, www.washingtonpost.com/blogs/federal-eye/wp/2015/08/17/irs-says-breach-of-taxpayer-data-far-more-widespread-than-it-first-thought-610000-taxpayers-at-risk/.

3. Devlin Barrett and Damian Paletta, "Officials Masked Severity of Hack," *The Wall Street Journal*, June 24, 2015, www.wsj.com/articles/hack-defined-as-two-distinct-breaches-1435158334.

4. iBridge, *7 Things About Medical Identity Theft Healthcare Executives Need to Know*, marketing.ibridgellc.com/acton/media/5746/7-things-medical-identity-theft-healthcare-executives-need-to-know.

5. Federal Trade Commission, "Medical Identity Theft," August 2012, www.consumer.ftc.gov/articles/0171-medical-identity-theft.

6. IRS, "Taxpayer Guide to Identity Theft," July 27, 2015, www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft.

7. IRS, "IRS IP PIN Pilot Continues in Georgia, Florida and the District of Columbia," January 27, 2015, www.irs.gov/uac/Newsroom/IRS-IP-PIN-pilot-continues-in-Georgia,-Florida-and-the-District-of-Columbia.

8. PURE, "Cyber Knowledge Center," www.puresituationroom.com/risks/cybersafe-knowledge-center/index.

9. *Ibid*.

10. Chief Executive, "Privacy/Data Security Remains the No. 1 Personal Risk Concerning Mid-Market CEOs," February 25, 2015, chiefexecutive.net/privacydata-security-remains-the-no-1-personal-risk-concerning-mid-market-ceos/.

About SignatureEXEC

As an executive, your business is running your company. At SignatureEXEC, our business is helping you manage your financial affairs. While you focus on your professional and personal responsibilities, we proactively design and help coordinate your finances so you can live the great life you envision.

For information about SignatureEXEC, please contact Dan Dubay, Partner and Director of SignatureEXEC, at dan.dubay@signaturefd.com.