Guarding Against Identity Theft

Presented by Paul Bonapart

When someone uses your name, credit card, social security number, or other financial information to commit a crime, you are a victim of identity theft. Luckily, you can take steps to make it more difficult for thieves to access your personal data.

What Is Identity Theft?

While stealing your wallet or mail is one tactic, thieves are just as likely to obtain your personal information from businesses you frequent. Or, using a technique called phishing, they may try to trick you into providing information by posing as your bank or a government agency. Once they have your key data, they can change your address with your credit card issuers, open up new credit cards in your name, drain your bank account, take out loans, apply for government-issued identification, or impersonate you during an arrest. They may even entangle your identity in a sophisticated fraud on a third party without your even knowing it.

How Will You Know Your Identity Has Been Stolen?

Because identity theft has become so prevalent, it pays to be aware. The first clue that your identity has been stolen is often a call from your credit card issuer about suspicious account activity. Or, you might notice you've stopped receiving credit card or bank statements. You might get a call from a business about merchandise or services you didn't order. Worse yet, you could be denied credit or receive a notice from a collection agency.

How Can You Combat Fraud?

Use the following tips to help keep your personal information safe from thieves:

- Keep a close eye on your credit by requesting a free credit report once a year. Call 877.322.8228 or visit www.annualcreditreport.com. (Don't be fooled by similar websites that are in the business of selling credit protection services.)
- You can freeze or secure your credit account at no cost with the three major credit bureaus: Equifax, Experian, and Transunion.
- Review your credit card and bank statements regularly (as often as weekly) for charges you didn't make. Some thieves will charge a small purchase to test if the account is active; if it goes through undetected, they'll move on to much larger purchases.
- Be smart about your passwords. Because it's relatively easy for thieves to obtain information about you from social networking sites, don't use your phone number, birthday, or names of your children or pets as passwords. Smart passwords include a combination of lowercase and uppercase letters, numbers, and symbols.
- Ask the businesses and institutions you work with (or for) about how they secure your information. "Dumpster diving" is a popular way for thieves to access information carelessly thrown away by businesses.
- Don't fall victim to a phishing scam. If you receive a call or an email that appears to be from a trusted institution or business, don't immediately provide identifying information. Instead, visit the business's website and call its customer service number. Or, if the message appears to be from your credit card company, call the number printed on the back of your card.
- Don't click on links within emails. Rather, type the URL directly into your browser's address line.
- Secure your mail. Before you travel, ask the post office to hold your mail until you return. Don't leave bill payments in an unsecured mailbox, and have reordered checks delivered to your bank rather than mailed to your home.
- Shred your credit card receipts, bank statements, and other documents that could provide a thief with your financial information.
- Don't carry your credit or debit cards in your wallet if you don't plan to use them. Never carry your social security number in your wallet.
- Update your computer's virus protection, and don't open email attachments from people or businesses you don't know.

- Install a firewall on your computer to thwart hackers.
- Look for the lock icon or “https” address when shopping online. Always log off when leaving a password-protected site.
- Use a wipe utility program before throwing away old computer equipment or smartphones.

If you suspect that your identity has been stolen, follow the steps provided on the Federal Trade Commission’s website at www.ftc.gov/idtheft.

What About Identity Theft Protection Services?
With cases of identity theft on the rise, many companies have entered the market with services promising to protect or minimize your risk. It’s important to keep in mind that the industry has its own share of fraudulent promoters of worthless services. Be sure to do your research and understand the level of protection the company offers.

This material has been provided for general informational purposes only and does not constitute either tax or legal advice. Although we go to great lengths to make sure our information is accurate and useful, we recommend you consult a tax preparer, professional tax advisor, or lawyer.

Paul Bonapart, JD, RFC, AIF®

Financial Security Planning Services, Inc.

520 Tamalpais Drive | Suites 103/104 | Corte Madera, CA 94925

415.927.2555 | 415.329.0071 fax | www.financialsecurityplanning.com | paul@financialsecurityplanning.com