BFS Wealth Management
8141 E. Kaiser Blvd.
Ste 300
Anaheim Hills, CA 92808
714-282-1566
contactus@bfsg.com
www.bfsg.com

Protect Yourself against Identity Theft

Two types of identity theft

- ***Account takeover*** *is what happens when a thief gets your existing credit or debit cards (or even just the account numbers and expiration dates) and goes on a shopping spree at your expense*
- ***Application fraud*** *is what happens when a thief gets your Social Security number and uses it (along with other personal information about you) to obtain new credit in your name*

Whether they're snatching your purse, diving into your dumpster, stealing your mail, or hacking into your computer, they're out to get you. Who are they? Identity thieves.

Identity thieves can empty your bank account, max out your credit cards, open new accounts in your name, and purchase furniture, cars, and even homes on the basis of your credit history. If they give your personal information to the police during an arrest and then don't show up for a court date, you may be subsequently arrested and jailed.

And what will you get for their efforts? You'll get the headache and expense of cleaning up the mess they leave behind.

You may never be able to completely prevent your identity from being stolen, but here are some steps you can take to help protect yourself from becoming a victim.

Check yourself out

It's important to review your credit report periodically. Check to make sure that all the information contained in it is correct, and be on the lookout for any fraudulent activity.

You may get your credit report for free once a year. To do so, visit www.annualcreditreport.com.

If you need to correct any information or dispute any entries, contact the three national credit reporting agencies: Equifax, Experian, and TransUnion.

Secure your number

Your most important personal identifier is your Social Security number (SSN). Guard it carefully. Never carry your Social Security card with you unless you'll need it. The same goes for other forms of identification (for example, health insurance cards) that display your SSN. If your state uses your SSN as your driver's license number, request an alternate number.

Don't have your SSN preprinted on your checks, and don't let merchants write it on your checks. Don't give it out over the phone unless you initiate the call to an organization you trust. Ask the three major credit reporting agencies to truncate it on your credit reports. Try to avoid listing it on employment applications; offer instead to provide it during a job interview.

Don't leave home with it

Most of us carry our checkbooks and all of our credit cards, debit cards, and telephone cards with us all the time. That's a bad idea; if your wallet or purse is stolen, the thief will have a treasure chest of new toys to play with.

Carry only the cards and/or checks you'll need for any one trip. And keep a written record of all your account numbers, credit card expiration dates, and the telephone numbers of the customer service and fraud departments in a secure place--at home.

Keep your receipts

When you make a purchase with a credit or debit card, you're given a receipt. Don't throw it away or leave it behind; it may contain your credit or debit card number. And don't leave it in the shopping bag inside your car while you continue shopping; if your car is broken into and the item you bought is stolen, your identity may be as well.

Save your receipts until you can check them against your monthly credit card and bank statements, and watch your statements for purchases you didn't make.

When you toss it, shred it

Before you throw out any financial records such as credit or debit card receipts and statements, cancelled checks, or even offers for credit you receive in the mail, shred the documents, preferably with a cross-cut shredder. If you don't, you may find the panhandler going through your dumpster was looking for more than discarded leftovers.

Keep a low profile

The more your personal information is available to others, the more likely you are to be victimized by identity theft. While you don't need to become a hermit in a cave, there are steps you can take to help minimize your exposure:

- To stop telephone calls from national telemarketers, list your telephone number with the Federal Trade Commission's National Do Not Call Registry by registering online at www.donotcall.gov
- To remove your name from most national mailing and e-mailing lists, as well as most telemarketing lists register online with the Direct Marketing Association at www.dmachoice.org
- To remove your name from marketing lists prepared by the three national consumer reporting agencies, register online at www.optoutprescreen.com
- When given the opportunity to do so by your bank, investment firm, insurance company, and credit card companies, opt out of allowing them to share your financial information with other organizations
- You may even want to consider having your name and address removed from the telephone book and reverse directories

Take a byte out of crime

Whatever else you may want your computer to do, you don't want it to inadvertently reveal your personal information to others. Take steps to help assure that this won't happen.

Install a firewall to prevent hackers from obtaining information from your hard drive or hijacking your computer to use it for committing other crimes. This is especially important if you use a high-speed connection that leaves you continuously connected to the Internet. Moreover, install virus protection software and update it on a regular basis.

Try to avoid storing personal and financial information on a laptop; if it's stolen, the thief may obtain more than your computer. If you must store such information on your laptop, make things as difficult as possible for a thief by protecting these files with a strong password--one that's six to eight characters long, and that contains letters (upper and lower case), numbers, and symbols.

"If a stranger calls, don't answer." Opening e-mails from people you don't know, especially if you download attached files or click on hyperlinks within the message, can expose you to viruses, infect your computer with "spyware" that captures information by recording your keystrokes, or lead you to "spoofs" (websites that replicate legitimate business sites) designed to trick you into revealing personal information that can be used to steal your identity.

If you wish to visit a business's legitimate website, use your stored bookmark or type the URL address directly into the browser. If you provide personal or financial information about yourself over the Internet, do so only at secure websites; to determine if a site is secure, look for a URL that begins with "https" (instead of "http") or a lock icon on the browser's status bar.

And when it comes time to upgrade to a new computer, remove all your personal information from the old one before you dispose of it. Using the "delete" function isn't sufficient to do the job; overwrite the hard drive by using a "wipe" utility program. The minimal cost of investing in this software may save you from being wiped out later by an identity thief.

Be diligent

As the grizzled duty sergeant used to say on a televised police drama, "Be careful out there." The identity you save may be your own.

IMPORTANT DISCLOSURES

BFS Wealth Management is neither a law firm nor a certified public accounting firm and no portion of the newsletter content should be construed legal or accounting advice. Each taxpayer should see independent advice from a tax professional based on his or her individual circumstances.

The information presented here is not specific to any individual's personal circumstances. Moreover, you should not assume that any discussion or information contained in this newsletter serves as the receipt of, or as a substitute for, personalized investment advice from BFS Wealth Management. Please remember to contact BFS Wealth Management, **in writing** , if there are any changes in your personal/financial situation or investment objectives for the purpose of reviewing/evaluating/revising our previous recommendations and/or services.

These materials are provided for general information and educational purposes based upon publicly available information from sources believed to be reliable - we cannot assure the accuracy or completeness of these materials. The information in these materials may change at any time and without notice.

A copy of our current written disclosures statement discussing our advisory services and fees continues to remain available for your review upon request.

Prepared by Broadridge Investor Communication Solutions, Inc. Copyright 2016