Coldstream

Financial success is just the beginning.

Our approach provides relevant, unbiased financial advice based on your distinctive needs to help you achieve your financial and lifestyle goals.

425.283.1600
800.665.1936
coldstream.com

One 100th Ave NE, Suite 102
Bellevue, WA 98004

Tips on Preventing Fraud

Unfortunately in our increasingly interconnected and automated world, we are seeing a big uptick in cases of fraud. While it is unlikely all cases may be prevented, there are several ways you can better protect yourselves and your information.

Coldstream offers this brief article on fraud prevention as a timely topic. While regrettably there is no current way for the IRS to alert you if a tax return has been filed fraudulently on your behalf, and many credit monitoring agencies only report on new account activities, there are still many steps we as consumers may take to protect ourselves.

Protect your Social Security Number.

Do not carry your Social Security card on you. If asked for your Social Security number, ask why it is needed and what will happen if you don't provide it. If your health plan or other type of ID card uses your Social Security number, request the company replace it with a different number. Routinely check your earnings record posted to your Social Security Statement. As paper statements are no longer being mailed each year, we recommend you sign up for online access at www.socialsecurity.gov/myaccount to create an account. Sometimes Social Security numbers are used by illegal workers or in error, so routinely checking the earnings the Social Security Office has compared to your actual earnings will highlight a potential problem. More information may be found on the Social Security webpage at www.ssa.gov.

Fight "phishing"—don't take the bait.

Scam artists "phish" for victims by pretending to be family members, banks, stores, government agencies, even the IRS. They do this over the phone, via emails and regular mail. A basic rule is do not give out your personal information unless you initiated the contact. Phishing emails sometimes have unprofessional language, spelling or grammar mistakes, and other attributes that are unlikely from reputable companies, but others are much more sophisticated. Even if the web address or email address looks legitimate, never follow requests to 'click on the link'; scam artists are excellent at creating emails and web sites that look legitimate but are actually fraudulent. Don't respond to a request to verify your account number or password. Legitimate companies would not request your information this way. In all cases, if in doubt, hang up the phone or delete the email and contact your financial institution directly.

Keep your identity from getting trashed.

Shred or tear up papers with personal information before you throw them away. Shred credit card offers, bills, bank statements and anything with your Social Security number on it. Consider signing up for online statements rather than paper copies or and even consider a PO Box or locking mail box to avoid having your mail compromised.

Coldstream_IdentityTheft_final_829.indd 1 8/29/14 7:07 AM

Control your personal financial information.

Check with your bank and other financial institutions about their policies on sharing your personal information. Rest assured Coldstream never shares personal information with third parties except as required by law.

Shield your computer from viruses and spies.

Protect your personal information on your home computer. Use strong passwords: with at least eight characters, including a combination of letters, numbers, and symbols. Good passwords are easy for you to remember but difficult for others to guess. Never use common and easily-guessed elements like birthdays, anniversaries, addresses, or names of family members. Use firewall, virus and spyware protection software that you update regularly. Steer clear of spyware. Download free software only from sites you know and trust. Don't install software without knowing what it is. Set your web browser's security settings to at least "medium." Don't click on links in pop-up windows or in spam e-mail. Never click on ads or pop-up windows claiming that your computer is infected with a virus—often these links will actually install spyware or viruses on your computer.

Click with caution.

When shopping online, check out a web site before entering your credit card number or other personal information. Read the privacy policy and look for opportunities to opt out of information sharing. (If there is no privacy policy posted, beware! It may be best to shop elsewhere.) Only enter personal information on secure web pages with "https" in the address bar and a padlock symbol at the bottom of the browser window. These are signs that your information will be encrypted or scrambled, protecting it from hackers.

Be cautious with Social Media

Avoid posting on Social Media when you will be away from home. While it is fun to share travel plans it alerts others that your home may be unattended. Set your profile to private so only invited contacts may see your information. However, remember if you are tagged in a photo all the contacts of the other people tagged may now see your information so if in doubt ask to have the tag removed.

Check your bills and bank statements.

Open your credit card bills and bank statements right away. Check carefully for any unauthorized charges or withdrawals and report them immediately. Call if bills don't arrive on time. It may mean that someone has changed contact information to hide fraudulent charges.

Stop pre-approved credit offers.

Stop most pre-approved credit card offers. They make a tempting target for identity thieves who steal your mail. Have your name removed from credit bureau marketing lists. Call toll-free 1-888-5OPTOUT (888-567-8688) or opt out online at www.optoutprescreen.com.

Ask questions.

Ask questions whenever you are asked for personal information that seems inappropriate for the transaction. Ask how the information will be used and if it will be shared. Ask how it will be protected. Explain that you're concerned about identity theft. If you're not satisfied with the answers, consider going somewhere else.

Check your credit reports—for free.

One of the best ways to protect yourself from identity theft is to monitor your credit history. You can get one free credit report every year from each of the three national credit bureaus: Equifax, Experian and TransUnion. Request all three reports at once, or be your own no-cost credit-monitoring service. Just spread out your requests, ordering from a different bureau every four months. Order your free annual credit reports by phone, toll-free, at 1-877-322-8228, or online at www.annualcreditreport.com.

We are your resource.

If you have any questions or concerns about potential fraud activity, please do not hesitate to contact Coldstream. We are happy to help and discuss the best options for you.

Coldstream_IdentityTheft_final_829.indd 2 8/29/14 7:07 AM