



John Weller
Vice President/Certified Mortgage Planner
Megastar Financial Corporation
Phone: 720.984.8972
Fax: 303.362.6705
License: NMLS 65428 CO 100020394
jw@megastarfinancial.com



Identity Theft: 5 Tips to Protect Your Privacy

The Federal Trade Commission (FTC) estimates that as many as 9 million Americans have their identities stolen each year. This means that an identity is stolen every 3 seconds, costing the average victim nearly \$4,000 and nearly 175 hours to straighten out their problems and their credit. How can you protect yourself from the dangers of identity theft? Here are some suggestions.

Conduct a Credit Check-up – Visit www.annualcreditreport.com to obtain a free credit report every 12 months. Review all three of your credit reports and look for any suspicious activity, unusual or inaccurate names or addresses, or any inquiries that were done without your knowledge. In many states, you may place a 90-day "Fraud Alert" on your credit report, which further restricts access to your credit information. Simply call one of the three main credit bureaus to activate the alert. Here are the toll-free numbers: Equifax 1-800-525-6285; Experian® 1-888-397-3742; or TransUnion® 1-800-680-7289.



Don't Give It Up – Avoid falling prey to phishing scams, both over the phone and through email. In a phishing scam, identity thieves pretend to be someone from your bank or a credit institution and simply ask you for your personal information. If someone contacts you and requests any personal information, don't give it to them. Verify who is requesting the data and why, and then call the institution yourself. One extra phone call could save you a lot of trouble and money.

Stay off the Pharm – While phishing enables thieves to pilfer information from you, pharming is another kind of scam that consists of hijacking your computer and stealing your personal information. A pharming site is designed to look just like the website you're trying to visit. However, enter your information on this fake site and not only can it track your moves within it, it may also direct your computer to give up other personal information at a later time. Be sure you are visiting the correct site, that the address in the navigation bar is correct before entering any information.

Return to Sender – Some scammers simply fill out a change of address form and divert your mail to another location. Others simply steal the mail they want right from your mailbox. The key to avoiding this scam is to know your statement delivery dates and pay close attention to any unusual delays in delivery. A lot of identity thieves do things the old-fashioned way: They rummage through your trash to collect your information that way. Be sure to shred any junk mail or other documents that may contain your personal information before you throw it away.

Opt-out of Special Offers – Visit www.optoutprescreen.com to cut down on the pre-approved offers from credit card and insurance companies. It's also good idea to have your clients opt out as well, especially if they're thinking about buying a home. When people apply for a mortgage, they often become "trigger leads" to the credit bureau, who sell your clients' information to any number of companies. It only takes a few minutes to opt out, but it could spare your clients a ton of junk mail and could possibly save them from identity theft.

Give me call. I have a great article on Trigger Leads you can give to your clients.

NMLS # 65428 Colorado MB License #100020394 To verify a mortgage loan originator license please visit:
<http://www.dora.state.co.us/real-estate/mortgagebrokerregistration.htm>

