How to Stay Safe From Identity Theft and Other Financial Crimes

Download the Top 25 Safety Tips at RishiKumar.com/Safety

Create an Online Social Security Account

- This prevents criminals from having your social security benefits sent to them.
- You can create this account at any age at www.ssa.gov, but it is especially important for those age 62 and older, as they are eligible to collect social security benefits and could be victimized.
- Creating an online account does not mean you have to start taking benefits, but it does help prevent fraud.

Freeze All Four of Your Credit Reports

- This prevents criminals from using your identity to open financial accounts.
- Freezing is the best option to protect your identity. It is free. Note that freezing is not the same as a lock, fraud alert or credit monitoring. See page 2 of this document for more information about freezing your credit reports.

Create an Internal Revenue Service Personal Identification Number

- This prevents criminals from filing a tax return in your name.
- You can get a PIN if you live in certain states, which the IRS is adding to overtime. Apply for your PIN at www.irs.gov if you are eligible, if not, continue to check for eligibility.

Protect Your Mail

- Criminals will steal outgoing mail and use it to commit fraud.
- Take any mail with sensitive information to the post office, including anything with a check enclosed. Criminals will steal checks and "wash" them, then write checks to themselves.
- Sign-up for USPS Informed Delivery, which provides you with pictures of the mail that you will be receiving.

Protect Your Trash

- Shred sensitive information with a cross-cut, diamond-cut or micro-cut shredder.
- Sign-up for e-delivery of bank statements and other documents. It will relieve you of the need to shred documents and save a few trees in the process.

Beware of Trick Phone calls

- Criminals can "spoof" your caller id and make it appear that the incoming call is from a different number.
- The caller may say they are with a government agency or a credit card company. They will ask you for sensitive information, which can be used to steal your identity or your money.
- The general rule is that you should never give information to people who call you.

Beware of Wire Transfer Scam

- This crime starts when the email of a title company, attorney, or real estate company is compromised.
- Emails are sent to homebuyers requesting wire transfers for a sale to be completed.
- To prevent fraudulent wire transfers, always contact the recipient of the wire by phone to verify the transfer instructions.

Prevent Home Title Fraud

- This crime occurs when a person fraudulently transfers the title of real property into their name.
- It can happen if the criminal knows how to access online deed records and make changes to the deed holder.
- To prevent this crime, check with your county records office to see if they have a notification system regarding attempted changes to deeds. If not, you should check the records yourself on a regular basis.

Don't Let Emotions Overcome Logic and Common Sense

- According to the FBI, each year Americans lose millions of dollars to various scams, most of which play on our emotions. Here are three of the most common scams:
  - Romance scam: Criminals pose as interested romantic partners on social media or dating websites to capitalize on their victims' desire to find companions. Most often, the target is asked to transfer money to the scammer.
  - Grandparent scam: Criminals pose as a relative—usually a child or grandchild—claiming to be in immediate financial need.
  - Sweepstakes/charity/lottery scam: Criminals claim to work for legitimate charitable organizations to gain victims' trust or they claim their targets have won a foreign lottery or sweepstake, which they can collect for a "fee."

Use Tools to Keep a Watch on Your Assets

- Create alerts on your financial accounts just in case an unauthorized person tries to withdrawal your money.
- You will be notified by text message or email when there are financial transactions in your accounts.
- The sooner you are aware of fraud, the easier it is to stop it and address the situation.

> "Identity theft is a new threat. Please safe guard yourself."
>
> Rishi Kumar,
> Candidate for the
> U.S. Congress CA-18

Tax Refund Fraud

Criminals can file tax returns using your identity. When this happens, you won't be able to file your tax return. Check with your state authorities to see what methods they use to help prevent fraud. For federal taxes, you might be able to get a PIN number from the IRS to prevent fraud. To see if you can, go to this site: www.irs.gov.

Social Security Benefits Fraud

With your social security number, a criminal can sign-up for social security benefits in your name or re-direct existing benefits to their bank account. Here is what to do: If you are 62 years of age or older and have not created your online social security account, prevent the criminal from doing it before you. Sign-up at www.ssa.gov.

Medical Fraud

IIf a criminal uses your identity to receive medical services, not only does it defraud the insurance provider or Medicare, but it could create entries in your permanent medical record for procedures you did not receive and conditions that you don't have. Here is what to do: Check your health insurance statements carefully and let providers know if you have been a victim of identity theft.

Title Fraud

Criminals use your identity to forge paperwork that transfers your real estate into their name. The transfer is not legitimate, because it is based on fraudulent documents. However, it is possible they could sell the property before the fraud is discovered. Your best defense here is to routinely monitor your property's records in the county. Check with your county to see if they offer automatic notification if there is a record change.

Steps to Take if You Are a Victim of Identity Theft

1. Freeze all four credit reports (contact information above). You can freeze your reports by phone, mail or online.
2. Call your local police and file a report.
3. Call the Social Security Administration's fraud hotline at 800-269-0271.
4. Contact the Internal Revenue Service at 1-800-829-0433.
5. Notify any organization that has your money, including financial advisors.
6. Notify your medical insurance providers.
7. Review all recent account statements for unauthorized activity and report any suspicious transactions to the business where the unauthorized or suspicious activity occurred.