Preventing Identity Theft

Presented by Retired
FBI Special Agent Jeff Lanza
Phone: 816-853-3929
jefflanza@thelanzagroup.com
www.thelanzagroup.com

1. **Protect Your Personal Information**
   - ✓ Don't carry your social security card. The key to identity theft is your social security number.
   - ✓ Don't provide your social security number to anyone unless there is a legitimate reason, which include occasions when you are: applying for employment; opening a financial account; getting a credit check; checking or freezing your credit reports.
2. **Protect Your Documents**
   - ✓ Shred your sensitive trash with a cross-cut, micro-cut or diamond-cut shredder.
   - ✓ Don't leave outgoing mail with personal information in your mailbox for pickup.
3. **Be Vigilant Against Tricks**
   - ✓ Never provide personal information to anyone in response to an unsolicited request.
   - ✓ Never reply to unsolicited emails from unknown senders or open their attachments.
   - ✓ Don't click on links in emails from unknown senders.
4. **Protect Your Communications**
   - ✓ Keep your computer and security software updated.
   - ✓ Don't conduct sensitive transactions on a computer that is not under your control.
   - ✓ Protect your Wi-Fi with a strong password and WPA2 encryption.
5. **Protect Your Digital World**
   - ✓ Use strong passphrases (passwords) with at least twelve characters.
   - ✓ Use different passphrases for your various online accounts.
   - ✓ Consider using password management programs. Or use the "Notes" app on your phone, as long as you secure the note with a password.

If They Have Your Social Security Number, Here's What Criminals Can Do With A Stolen Identity

- New account fraud – meaning that they open credit card accounts, bank accounts and get loans in your name
- File state and federal tax returns in your name
- File for social security benefits in your name (if you're eligible), or redirect benefits to their account
- Get medical care or prescription drugs in your name

Options You Have To Prevent New Account Fraud

1. **Fraud Alert:** Your credit file at the four credit reporting agencies is flagged and a potential lender should take steps to verify the identity of a person opening a new account. ***Inside Scoop:*** *Not worth the effort. Fraud alerts only work if the merchant takes steps to* verify the identity of the applicant. *They expire automatically after one year or seven years if you have been a proven victim of identity theft.*
2. **Credit Lock**: Limits access to your credit reports by some parties without your approval. ***Inside Scoop:*** *Don't use this. Locks are not governed by federal law, there is no guarantee of error free operation and some credit reporting agencies may charge you a monthly fee for this service.*
3. **Credit Monitoring:** Your credit files are monitored and if activity occurs, you are notified. ***Inside Scoop:*** *Credit monitoring does not prevent fraud it only notifies you when your credit reports have been accessed. In most cases, the monitoring companies provide resolution services, which can be very beneficial.*
4. **Credit Freeze:** A freeze restricts access to your credit reports and should prevent new account activity in your name. This requires unfreezing (lifting) before you can open a new account. ***Inside Scoop:*** *This is highly recommended and is a proven way to protect against new account fraud. As of September 2018, it is free to freeze your credit reports and to create and freeze credit reports for minors in every state.*

Credit Reporting Bureaus			
	Experian: (888) 397-3742 P.O. Box 9530 Allen, TX 75013 **www.experian.com/freeze**	You can freeze credit reports by mail, phone or online.	**Innovis:** (800) 540-2505 P.O. Box 1640 Pittsburgh, PA 15230 **www.innovis.com/personal/securityFreeze**
	Equifax: (800) 685-1111 P.O. Box 740241 Atlanta, GA 30374 **www.equifax.com/personal/credit-report-services**		**Trans Union:** (888) 909-8872 P.O. Box 2000 Chester, PA 19016 **www.transunion.com/credit-freeze**

You are allowed 4 free reports each year. To order three: www.annualcreditreport.com or 877-322-8228; Your credit report at Innovis must be ordered from: www.innovis.com/personal/creditreport

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

If 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 which 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.

Help to stop robocalls with **Robokiller** phone app. **Nomorobo** can be used for landlines connected to the internet.

To remove your name from lists:
Mail - www.dmachoice.org; **Phone -** www.donotcall.gov
To stop credit card offers and other solicitations:
www.optoutprescreen.com ***or*** 1-888-5-OPTOUT (567-8688);

Key Resources
Police or FBI: Search online for local number
FTC: 1-877-IDTHEFT; www.identitytheft.gov
To Report Internet Fraud: www.ic3.gov