CONSUMER NEWS
SAN DIEGO CITY ATTORNEY'S OFFICE

Taxpayer Identity Theft

April 2013

Taxpayer identity theft occurs when someone uses the personal identifying information of another person to file a tax return and claim a refund. This newsletter offers tips to prevent you from becoming a victim of taxpayer ID theft and explains the steps to take if your identity is stolen.

ALERT - POSSIBLE TAX FRAUD

The Internal Revenue Service (IRS) wants taxpayers to be alert to possible identity theft. If a taxpayer receives any of the following notices or letters from the IRS they should be concerned:

- More than one tax return was filed for you
- You have a balance due, refund offset or have had collection actions taken against you for a year you did not file a tax return
- IRS records indicate you received wages from an employer unknown to you

WHAT TO DO IF YOU SUSPECT TAXPAYER ID THEFT

If you receive a notice by mail from the IRS that leads you to believe your identity has been used by someone else, the IRS wants you to contact them immediately. The IRS Identity Protection Specialized Unit can be reached at 1-800-908-4490. You may need to fill out the IRS Identity Theft Affidavit, Form 14039, which is available at www.irs.gov. (This is the only official IRS web address.)

GUARDING YOUR PERSONAL INFORMATION:

To avoid becoming a victim of taxpayer identity theft, take the following steps to safeguard your personal information:

1. The IRS does not initiate contact with taxpayers by email to request personal or financial information. If you believe you have received a phony IRS email, forward it to the IRS at phishing@irs.gov.

2. Do not respond to any emails requesting personal information, as they may be from companies posing as an accounting or tax preparation business with whom you deal. (This is called phishing.)

3. Don't give personal information over the phone, through the mail or on the Internet unless you have initiated the contact or you are sure you know who you are dealing with.

4. Don't give a business your SSN just because they ask. Give it only when required.

5. Do not carry your Social Security card, or any other document with your SSN, in your wallet.

6. Keep your personal information in a secure place.

7. Shred documents that contain personal information, using a cross-cut shredder, when you no longer need them.

8. Do not put your outgoing mail in your unsecured mailbox for pickup. Deposit mail in a post office collection box.

9. If your mailbox is unattended during the day, consider getting a post office box or a locking mailbox.

10. Install firewalls and virus protections on your home computers to prevent internet hackers from getting your private information.

STEPS TO TAKE IF YOUR INFORMATION IS STOLEN:

If you lose your wallet or find out that someone has used your identity, immediately take the following steps:

1. Report the theft to the local police agency. You can report the information to the agency where you live, even if the person who took your wallet or information is in another city or country. Get a copy of the police report. You may need it to take the other steps below.

2. Contact your credit card companies to report the theft (or loss) and to cancel your accounts. The companies will issue you new cards with new account numbers.

3. Place a fraud alert on your credit reports by contacting one of the three credit reporting companies. Each company is required to contact the other two companies. The contacts are:

- Equifax (800) 525-6285 or www.equifax.com
- Experian (888) 397-3742 or www.experian.com
- TransUnion (800) 680-7289 or www.transunion.com

Once you place the fraud alert in your file, the companies are required to provide you with a free copy of your credit report.

There are two types of fraud alerts:

- Initial alert—lasts for 90 days—use if your information has been lost, but no one has yet used the information
- Extended alert—lasts for 7 years—use when your information has been used by another person to obtain goods or services

The alert informs anyone who checks your credit that your information has been compromised and the business should take extra steps to verify the identity of the person applying for credit in your name.

4. File a complaint with the Federal Trade Commission at 1-877-IDTHEFT (1-877-438-4338). This allows the FTC to provide the information to the necessary law enforcement offices, which may lead to the arrest of the thief.

LOCAL PROSECUTION:

Our local law enforcement community is actively prosecuting identity thieves. By reporting theft to the police, you provide the law enforcement agencies with the information we need to bring these thieves to justice.

ADDITIONAL RESOURCES:

Consumers in San Diego have an excellent resource to assist with privacy questions and identity theft. The Identity Theft Resource Center helps victims of identity theft, at www.idtheftcenter.org. The Federal Trade Commission maintains a website with helpful information on identity theft at www.ftc.gov.

San Diego
City Attorney's Office
Consumer and Environmental Protection Unit
(619) 533-5600

Newsletter written by Kathryn Lange Turner

To report violations of consumer protection laws, call the City Attorney's Hotline at **(619) 533-5600.**