City of Roseville Police Department

911 Public Safety Newsletter

February 2018

Identity theft

Source: Federal Trade Commission (FTC), U.S. Department of Justice

What is identity theft?

According to the U.S. Department of Justice, identity theft (or fraud) is a term used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.

In 2017 Equifax had a data breach that exposed 143 million American consumers' personal information. If you have a **credit report**, there's a good chance that you were a victim of this data breach. As a result you may be or become a victim of ID theft.

Unfortunately, once the thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new accounts, or get medical treatment on your health insurance.

Here are a few precautions you can take if you think your personal information was compromised.

- **Check your credit reports** from Equifax, Experian, and TransUnion for free at **annualcreditreport.com**. Accounts or activity that you don't recognize could indicate identity theft. Visit **IdentityTheft.gov** to find out what to do.
- **Consider placing a credit freeze on your files.** A credit freeze makes it harder for someone to open a new account in your name. Keep in mind that a credit freeze won't prevent a thief from making charges to your existing accounts.
- **Monitor your existing credit card and bank accounts closely** for charges you don't recognize.
- If you decide against a credit freeze, **consider placing a fraud alert on your files.** A fraud alert warns creditors that you may be an identity theft victim and that they should verify that anyone seeking credit in your name really is you.
- Visit **Identitytheft.gov/databreach** to learn more about protecting yourself after a data breach.

Tax identity theft

Source: Federal Trade Commission (FTC)

Are you looking forward to getting your tax refund this year? Tax identity thieves may be looking forward to getting your refund too.

Tax identity theft happens when someone uses your Social Security number to get a tax refund or a job. You might find out it has happened when you get a letter from the IRS saying more than one tax return was filed in your name, or IRS records show you have wages from an employer you don't know.

The IRS uses your Social Security Number (SSN) to make sure your filing is accurate and complete, and that you get any refund you are due. Identity theft can affect how your tax return is processed. An unexpected notice or letter from the IRS could alert you that someone else is using your SSN. However, the IRS doesn't start contact with a taxpayer by sending an email, text or social media message that asks for personal or financial information. If you get an email that claims to be from the IRS, do not reply or click on any links. Instead, forward it to **phishing@irs.gov.**

If someone uses your SSN to file for a tax refund before you do, the IRS might think you already filed and got your refund. When you file your return later, IRS records will show the first filing and refund, and you'll get a notice or letter from the IRS saying more than one return was filed for you.

If someone uses your SSN to get a job, the employer may report that person's income to the IRS using your SSN. When you file your tax return, you won't include those earnings. IRS records will show you failed to report all your income. The agency will send you a notice or letter saying you got wages but didn't report them. The IRS doesn't know those wages were reported by an employer you don't know.

The FTC has these tips to fight tax identity theft:

- File your tax return early in the tax season, if you can.
- Use a secure internet connection if you file electronically, or mail your tax return directly from the post office.
- Respond to all mail from the IRS as soon as possible.
- If tax identity theft happens to you, visit **IdentityTheft.gov** to report it to the FTC, file an Identity Theft Affidavit with the IRS electronically, and get a personal recovery plan.

Protect your mail

It's tax season, and tax forms with sensitive financial information are being mailed. Thieves look for such documents to steal your identity and commit fraud. Make it a habit to empty your mailbox every day, as soon as possible after delivery. Never let mail sit in the mailbox overnight. If you're going on vacation, have the post office hold your mail until you return. For outgoing mail, we recommend handing your mail to the carrier or taking it to the post office for mailing.

Call police immediately if you see someone tampering with or prying a mailbox. Call 911 to report a crime in progress, or (916)774-5000 ext. 1 to report something after the fact.

Informed Delivery® by USPS®

Digitally preview your mail and manage your packages scheduled to arrive soon! Informed Delivery allows you to view greyscale images of the exterior, address side of letter-sized mail pieces and track packages in one convenient location. Sign-up for free at **USPS.com**.

CITY OF ROSEVILLE CALIFORNIA

New Medicare cards are coming

Medicare will mail new Medicare cards between April 2018 and April 2019. New cards will have a new Medicare Number that's unique to each member, instead of a Social Security Number. This will help to protect your identity.

Things to know about the new Medicare card

- The new card will automatically come to you. You don't need to do anything.
- Your Medicare coverage and benefits will stay the same.
- Your new card is free – there's no charge for it.

Watch out for scams

Medicare will never ask you to give personal or private information to get your new Medicare Number and card. Scam artists may try to get personal information (like your current Medicare Number) by contacting you about your new card. If someone asks you for your information, for money, or threatens to cancel your health benefits if you don't share your personal information, hang up and call 1-800-MEDICARE (1-800-633-4227).

Even if you are not currently on Medicare, you probably know some that is like your parents or grandparents. Inform them of possible scams that may occur with the issuing of the new Medicare card.

Here are a few tricks that criminals may use:

- A scam artist calls and claims to represent Medicare. They may tell you they need to confirm your Social Security number so they can send you the new card. Or they may ask you to verify other personal information.
- They may also use scare tactics, such as saying your Medicare benefits will be cancelled if you don't share the information.
- They could also ask for your credit card number, or tell you to wire money or buy gift cards, to pay for the new card.

These are all scams.

Avoid scams in 2018

Better Business Bureau (BBB)

Make these resolutions and give scams a miss

Scammers are constantly devising new tricks and refining old ones. However, no matter what cons emerge this year and beyond, follow these tried and true tips from the Better Business Bureau (BBB) to keep you safe.

1. **Keep your computer programs up-to-date**: Those reminders to update your Internet browser, operating system and other software are annoying, but don't ignore them. Keeping your programs current is a great defense against malware. Software manufactures continually update their programs to protect against the latest viruses.
2. **Set tough passwords.** To create strong passwords, combine lowercase and capital letters with a mix of numbers and symbols. Go ahead and write your passwords down, but don't store this cheat sheet on your computer.

3. **Keep your smartphone safe.** Take the same precautions on your mobile device as you do on your computer. Protect your phone with a passcode, keep your software up-to-date and watch out for malware disguised as apps.
4. **Know the telltale signs.** A little common sense goes a long way in spotting scams. Watch out for anything that's too good (or sensational) to be true. This covers everything from "free" gift cards to instant job offers to scandalous celebrity videos. And be skeptical of any communications riddled with typos and poor grammar. If it looks like a scam, it probably is.
5. **Don't act immediately... research first**. Most scams urge you to act right now, before you've had a chance to consider your options. Always be sure to do your research. Depending on the occasion, this can be anything from getting three contractor quotes to performing a quick online search. Just don't be pressured into a commitment before doing your homework.

Is this a scam?

(Federal Trade Commission, FTC)

Here's one of the top questions people ask the FTC. Is this a scam? Whatever the "this" looks like, here's the best answer to that question: Did someone say you can only pay by wiring money, putting money on a gift card, or loading money on a cash reload card? If they did, then yes: that is a scam.

Whether someone tells you to pay to claim a prize, help someone out of trouble, or deal with tax issues from the (so-called) IRS: nobody legitimate is ever going to say you have to pay by wiring them money, getting iTunes cards, or putting money on a MoneyPak, Vanilla Reload, or Reloadit card.

If anyone ever insists you pay in one of those ways, **tell the FTC**.

www.consumer.ftc.gov/blog/2018/01/how-scammers-make-you-pay

Sources: *Federal Trade Commission, U.S. Department of Justice, Medicare.gov, Better Business Bureau*

Police Department
1051 Junction Blvd.
Roseville CA 95678
(916) 774-5000
www.roseville.ca.us/police

Call 9-1-1
EMERGENCY
IN PROGRESS

Non-Emergency
(916) 774-5000 x 1

Abandoned Vehicle Hotline
(916) 746-1022

Alarms/Alarm Permits
(916) 774-5093

Animal Control
(916)774-5090

Community Events & Neighborhood Watch
(916) 774-5050
PDCommunityServices@roseville.ca.us

Graffiti Abatement
(916) 746-1021

Police News & Crime Alert Emails:
www.roseville.ca.us/enotify

RCONA
(Roseville Coalition Of Neighborhood Associations)
www.RCONA.org

Follow us on social media:

CITY OF ROSEVILLE CALIFORNIA

The "9-1-1" is published for City of Roseville's residents by the Community Relations Division of the Roseville Police Department. Please send comments or suggestions to: **pdcommunityservices@roseville.ca.us**, (916) 774-5050.

Vol. 18 Issue 2