CRIME ADVISORY

SCAMS AND HOW TO ADDRESS THEM

There are numerous tricks criminals use to get money or property from you. Their tactics and approaches change often. If you have become a victim of check fraud, bank card or credit card fraud, immediately report the incident(s) to the financial institution and request a new account be issued. **Also, all three credit bureaus offer a credit freeze free of charge.**

If you are or suspect you are being scammed, please call the **Sheriff's Department's non-emergency line** to file a report:

714-647-7000 or 949-770-6011

Text Phishing Scheme

The suspects in this scam are targeting disability applicants and beneficiaries by sending them text messages on their cellphone asking them to call. The text messages have read, “Disability Alert: Please call 253-xxx-xxxx regarding your recent disability benefits application.” The numbers to call have varied but the wording has been about the same. When the number is called a person claiming to be a Government official asks for personal identifying information. We have received reports of identity theft where victims have fallen for this scam.

Facts related to this scam:

- Social Security never sends unsolicited text messages.
- Once you give anyone your personal information, they can use it repeatedly or sell it for others to use.
- More information on this scam is available on the **Social Security Administration Office of the Inspector General website**.

What you can do to combat this scam:

- Never blindly respond to a text message by calling the number given. Do some research and find the actual number for the entity you are trying to call.
- Call the agency the person is from directly to verify their identity. Social Security has a toll-free number to call: **1-800-772-1213.**

- Report the scam to the Social Security Fraud Hotline at **https://www.oig.ssa.gov/report** or by phone at **1-800-269-0271**.
- If you are the victim of identity theft, take these steps after you have filed a report with your local law enforcement agency:
    1. Place a fraud alert with the credit reporting agencies and provide them with the police report number.
    2. Obtain a copy of your credit report and review it to make sure no accounts have been opened without your authorization. Dispute any accounts you did not authorize.
    3. Check the inquiry section of your credit report and make sure you made them. Call the telephone number listed for the ones you do not recognize and ask them why they ran your credit.

Online Employment Scam

The suspects in this scam either post an advertisement online offering employment or respond to your online solicitation. They almost always communicate with you via text message or email and involve several different variations. They will either send you a check that they want you to cash, or they will ask for your account information to deposit money into your account. They will then ask you to send them money via prepaid credit cards or they will have you wire them money. It can take banks several days or more to determine that the checks or deposits are fraudulent, and, in the meantime, you have given your money to the suspect. Your account will be charged for the full amount of the check or deposit plus fees.

Another variation of this scam is where the suspect sends you a check in the same manner as above then instructs to you buy merchandise or use a service acting as a “Secret Shopper”. In the end, you still end up sending money or merchandise to the suspect and you are at a loss once your bank determines is fraudulent.

Still another version of this scam deals more specifically with people who advertise online offering childcare. The premise is the suspect is moving to your area and needs someone to care for their wheelchair bound child. They send a large check for wages and costs related to the wheelchair. They want you to cash the check and then send the money to some third party (which is probably another alias of theirs) in order to either purchase the wheelchair or have it shipped. Once again, when the bank determines the check or deposit is fraudulent, your account will be charged for the full amount plus fees.

What you can do to combat this scam:

- Never follow a link on an unknown email or website unless you know where it will lead you. If you allow your cursor or arrow to hover over a link, then the true destination will appear in a text box.

- Avoid speaking to people using only text or email. Ask to speak with them in person or over the telephone. Be suspicious of people who will not do this or give you excuses why they cannot.
- If you suspect a check is fraudulent then take it to the issuing bank to verify it or at least telephone the bank. You can also try calling the business or person who is listed as the account holder on check.
- Report the scam to the **Federal Trade Commission (FTC)**.

Tech Support Scam

The suspects in this scam call you and claim they are from Microsoft Tech support. They talk you into allowing them control of your computer to fix a problem. In some cases, they also charge a fee which requires you to give them your credit card number. They will then ask for as much personal information as you will give them because they claim they need it to process the transaction.

Facts related to this scam:

- Microsoft does not make unsolicited phone calls.
- Once you give them control of your computer, they are free to obtain any information contained on it as well as place malicious software on it.
- Most merchants only need your name, card number and billing address to process a credit transaction. Some may need the three-digit security code from the back of the card.
- Merchants do not need to know your birthdate, social security number, mother's maiden name, etc. in order to process a credit transaction.

What you can do to combat this scam:

- Don't call them back or hang up if you are talking to them
- Contact Microsoft directly or visit their scam website: **https://www.microsoft.com/en-us/safety/online-privacy/avoid-phone-scams.aspx**
- Report the scam to the Federal Trade Commission (FTC). Information on how to do this is on their website: **https://www.consumer.ftc.gov/articles/0076-phone-scams**
- Report the scam to the Orange County Sheriff's Department by calling **714-647-7000** or **949-770-6011**

Telephone Taxes Due Scam

Someone calls or leaves a message on your answering machine stating you owe taxes. You answer the call or call the number back and the person threatens you with arrest, deportation, etc. if you do not pay the tax immediately. They then instruct you to obtain a prepaid credit card and give them the card number from the front of the card and the code from the back of the card. If you refuse most times another person will call you purporting to be from a local law enforcement agency threatening to arrest you if you do not pay. The caller ID number is most often "spoofed" so that it shows the number for the law enforcement agency.

Facts related to this scam:

- If you provide the numbers for the prepaid credit card, then the person can access the funds anywhere in the world.
- The IRS always sends taxpayers written notification of any tax due via the US mail.
- The IRS will never ask for credit card, debit card or prepaid card information over the telephone.
- The Orange County Sheriff's Department does not work in conjunction with the IRS for tax collection purposes.

What you can do if you get one of these telephone calls:

- Don't call them back or hang up if you are talking to them.
- If you know you owe taxes or you think you might owe taxes, call the IRS at **1-800-829-1040**. The IRS employees at that line can help you with a payment issue, if there really is such an issue.
- If you know you don't owe taxes or have no reason to think that you owe any taxes (for example, you've never received a bill or the caller made some bogus threats as described above), then call and report the incident to the Treasury Inspector General for Tax Administration at **1-800-366-4484**.
- If you've been targeted by this scam, you should also contact the Federal Trade Commission and use their "FTC Complaint Assistant" at **https://www.FTC.gov**.
- Please add "IRS Telephone Scam" to the comments of your complaint.
- Call the Orange County Sheriff's Department at **714-647-7000** or **949-770-6011** to verify whether an actual Sheriff's employee is calling you and to file a report.
- Visit the IRS website for further information at www.irs.gov and select Tax Scams, then telephone scams or follow this link: **http://www.irs.gov/uac/Newsroom/IRS-Reiterates-Warning-of-Pervasive-Telephone-Scam**.

Telephone Utilities Due Scam

This uses the same premise as the tax due scam, but the person threatens to have your utility turned off. They demand that you obtain a prepaid credit card and provide them with the numbers.

Facts related to this scam:

- If you provide the numbers for the prepaid credit card, then the person can access the funds anywhere in the world.
- Most utility companies allow for many forms of payments and never require just one.
- The Orange County Sheriff's Department does not work in conjunction with Utility Companies for the collection of money.

What you can do if you get one of these telephone calls:

- Don't call them back or hang up if you are talking to them.
- Contact your utility company immediately to verify.
  Southern California Edison **1-800-655-4555** or **https://www.sce.com**
  San Diego Gas & Electric **1-800-411-7343** or **https://www.sdge.com**
- Call the Orange County Sheriff's Department at **714-647-7000** or **949-770-6011** to verify whether an actual Sheriff's employee is calling you and to file a report.

Item Listed for Sale Check Scam

There are many variations of this scam and many different advertisement modes have been targeted but most lately have been through craigslist. The basic premise is that you list something for sale and the person contacts you to make the purchase. They come up with a story that makes you believe they have a legitimate check coming to you for more than what you are asking. They instruct you to cash the check, take the money out for the purchase, keep money for your trouble and then ultimately send them some amount of money immediately by prepaid credit card or wire. It can take banks several days or more to determine a check is fraudulent and, in the meantime, you have given your money to the suspect. Your account will be charged for the full amount of the check plus check fees.

What you can do to combat this scam:

- Deal locally with people you can meet with.
- Take the check you receive directly to the issuing bank and explain the circumstances to the teller.
- Report instances of this scam directly to listing company.
  Craigslist **http://www.craigslist.org/about/scams**
  Ebay **https://www.paypal.com/us/webapps/helpcenter/helphub/home/**.

- Call the Orange County Sheriff's Department at **714-647-7000** or **949-770-6011** to file a report.

Warrant for your Arrest Scam

The suspects in this scam call you, identify themselves as law enforcement officers and then direct you to pay a bail or fine to prevent arrest. The reasons for the warrant vary and most recently have been because you supposedly did not report for jury duty. They most often "spoof" the caller ID number to show the number or name of a local law enforcement agency. As with the other scams the suspects instruct you to obtain a prepaid credit card and give them the card number from the front of the card and the code from the back of the card.

Example of call generated in our City: Victim of fraud revealed she received a phone call from a subject who identified himself as **OCSD employee**. This subject informed the victim she had an outstanding warrant for her arrest with a bail of $8000.00. The victim indicted the phone number she received the phone call from was the number posted on our website for the OCSD Civil Bureau. The subject directed the victim to do the following:

- Sign up for Apple Pay and pay the bail amount (she was in the process to do so) or
- Get cash and drive to the Civil Bureau (the subject provided her with the address) to pay the bail amount.

The victim did not send any money and immediately filed a police report.

Facts related to this scam:

The Orange County Sheriff's Department will never demand payment for a warrant over the telephone.

- Payments related to warrants are handled through the Court that issued the warrant.
- You will never be restricted to one form of payment.
- If you provide the numbers for the prepaid credit card, then the person can access the funds anywhere in the world.

What you can do to combat this scam:

- Don't call them back or hang up if you are talking to them.
- Call the Orange County Sheriff's Department at **714-647-7000** or **949-770-6011** to determine if an OCSD employee is calling you and to file a report.
- Contact the court directly to inquire about bail or fine payment. The link **https://www.occourts.org/locations** contains court locations and contact information in Orange County.

OTHER SCAMS:

Mail Theft

Criminals are targeting stand-alone mailboxes in front of the US Post office and are “fishing” mail out of the mailbox. When they can obtain envelopes containing checks, the criminals are removing the Pay to the Order of name and changing it to another name to be cashed, which is commonly known as check washing. It is recommended to use gel pen when writing checks to combat check washing. If you are a victim of check washing, contact your bank immediately.

Example of call generated in our City: Victim reported an unknown suspect walked into a credit union in Las Vegas and cashed a check associated to one of her closed bank accounts. Unknown how the suspect obtained a check associated to that respective account. The check was cashed in the amount of $7,400 but victim did not incur any loss as the bank accepted her claim the transaction was fraudulent

Additional example of call generated in our City: Victim reported unknown suspect(s) fraudulently obtained his personal identifying information and attempted to make online purchases in his name. The transactions were unsuccessful and there was no loss.

Grandparent Scam

Individuals are calling the senior citizens of Orange County and telling the victim their grandson or granddaughter have been arrested. The individual on the phone tells the grandparent they need to wire money or obtain gift cards to bail out their grandchild from jail and/or to pay for a lawyer. The caller will attempt to keep the victim on the phone until the transaction has been completed. You should NEVER send wire money or purchase a gift card and provide the information to anyone on the phone. To prevent this scam, hang up and call your grandchild to ensure their safety.

New Crypto Payment Scam

Someone might call pretending to be from the government, law enforcement, a local utility company, a romantic interest met online, or information on winning the lottery. The caller will remain on the phone to direct the victim to withdraw money at a store with a cryptocurrency ATM. The caller will direct the victim to insert money into the ATM and buy cryptocurrency and send the victim a QR code with their address embedded in it. Once the cryptocurrency is purchased, the caller directs the victim to scan the QR code, so the money gets transferred to them.

Example of call generated in our City: Victim reported that he received a phone call from someone claiming to be a rep of Coinbase where he holds a crypto account. The caller asked the victim to log into his account and when he did, he was immediately locked out. The victim witnessed all $127,000 being transferred from his Coinbase account and into another unknown account.

Kidnapping Scam

In this scam, the victim receives a phone call and when they answer the phone call the victim will hear a cry for help. Generally, the victim will say a child's name to see if their child was calling them. With that information, the suspect will inform the victim they have kidnapped their child and is demanding money for their release. The suspect will keep the victim on the phone and give the perception that if the call disconnects then harm will happen to their loved one. The suspect will instruct the victim to wire cash out of the country and when completed the call will disconnect. The victim will call their loved one and determine they have been scammed out of their money through fear.

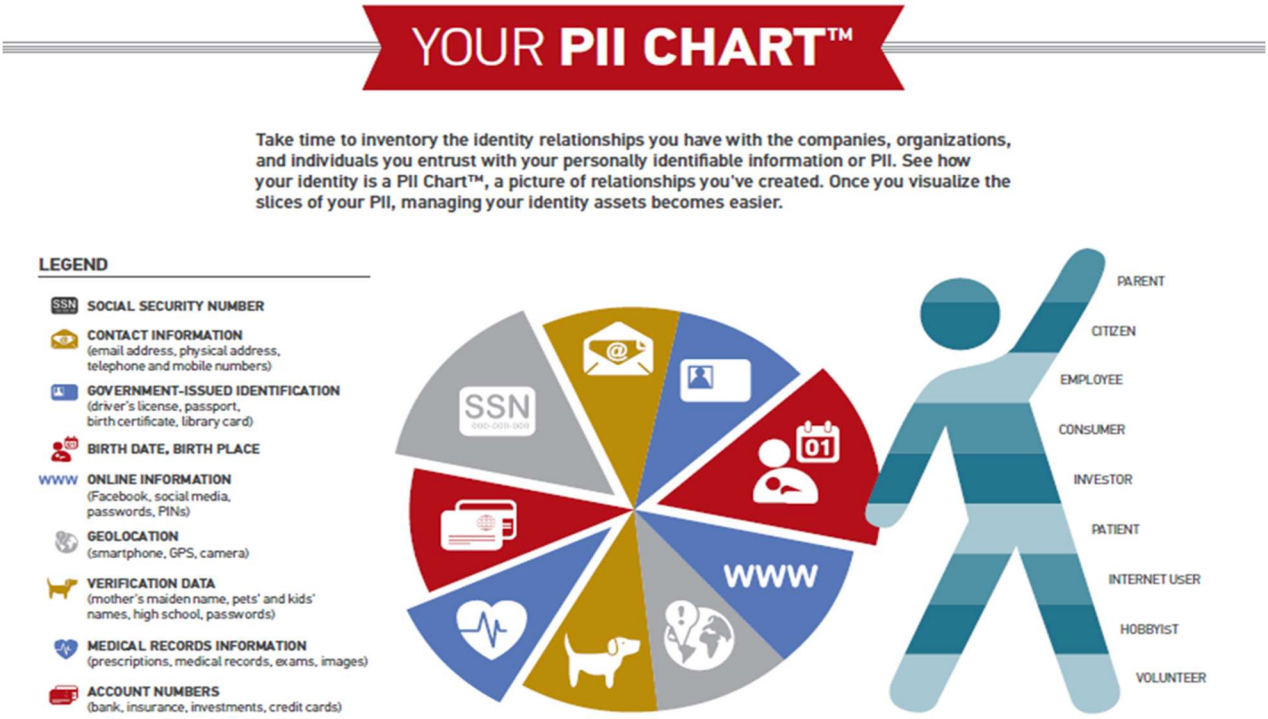
Craigslist Scam

When advertising an item for sale on a website or mobile app, scammers will contact the victim and tell the victim they are interested in purchasing their item. The suspect is never able to meet the victim to pick up the item, instead they will send a check for the item and for shipping. The check sent is usually a lot more money than the item that was for sale. The suspect relies on the victim to contact them about the extra money. When the victim contacts the suspect, the suspect will ask the victim to send money to the moving company, who will then come and pick up the item. If the victim sends money to the shipper prior to the check clearing, the victim will discover the initial check was a bad check and the funds were removed from their account.

Romance Scam

Victims of a romance scam generally meet the suspect online through a dating website. The suspect will establish a relationship with the victim, but the suspect is never able to meet the victim. This scam involves the suspect telling the victim they have some type of emergency or need to borrow money for a failing business or medical procedure. Once the money is sent, the suspect will continue with the relationship and try to obtain more money due to the established trust between the victim and the suspect. Eventually the victim will figure out that the relationship was established for fraud purposes and no money will ever be returned.

What is Personal Identifying Information (PII)



How is this information obtained?

From businesses and other institutions

- Access to on-the-job records or information
- Computer hacking
- “Dumpster Diving”
- Skimming/Shimming Devices
- The “Dark Web”

From your home:

- Mail theft
- Residential burglary
- “Dumpster Diving”
- Pre-Approved Credit Cards

What can Thieves do with your personal information?

- Open new credit card accounts

- Establish new utilities
- Open new checking accounts
- Counterfeit checks and credit/debit cards
- Access and drain your bank accounts
- Make large purchases with your credit history
- Use your identity to obtain a job
- Use your identity when arrested or given a citation
- Sell your identity on the Dark Web ($0.14 an identity!)

How to prevent it:

- Shred anything that has personal information
- Be “mail conscious,” shred everything
- Check your credit report, bank and credit card statements regularly
- Do not click on email links and allow others to access your computer
- If you didn’t initiate the call – don’t give out personal information. Hang up.
- Don’t respond to e-mails asking for personal information
- If you didn’t play the Nigerian or Canadian lotto- YOU DID NOT WIN!!
- Don’t share personal