Revision 20240729

ID THEFT, FINANCIAL FRAUD & SCAM REMINDER TIP SHEET

REMEMBER: These criminals are very sophisticated, both technologically and psychologically. Worldwide, there are tens of thousands of entire groups of people with extensive education and backgrounds in sales, marketing, finance, banking, computers, psychology, sociology, neuro-linguistic programming (NLP), etc. – everything needed to understand how our minds work, what "trips our triggers," and how best to convince us to give them money or for them to scam us in some manner or form. Personal loss estimates range from $20-$50 BILLION from 50+ million people annually in the U.S. alone and globally it's hundreds of millions of people affected and over $5 TRILLION, but it could be much worse as much of this crime goes unreported simply because people are ashamed to admit to family, friends, and law enforcement that they got scammed. Posting your personal information on social media only makes you even more of a target by giving them more information and avenues with which to attack you. STOP POSTING EVERYTHING ABOUT YOUR LIFE FOR THE ENTIRE PUBLIC TO SEE – CRIMINALS *WILL* USE ALL THAT INFORMATION AGAINST YOU!!! So, no matter who you are, your age, educational level or socio-economic status, these kinds of crimes affect everyone – 1 person or business every 3 seconds!!! If you suspect you have been scammed or are being abused or exploited, financially or otherwise, please, do not be afraid or ashamed to ask for help – it is not your fault this has happened to you! Our financial institutions and law enforcement recognize that these are serious crimes and they sincerely want to help stop them, but YOU MUST take steps to educate and protect yourself from this type of crime and report it immediately when it happens. YOU must be your own first responder in ALL aspects of your life!!!

In addition to reporting any crimes to the police and your financial institutions, go to the websites below immediately if you have been a victim – these websites outline everything you need to do to recover and protect yourself and your assets. Time (usually within 72 hours max.) is truly of the essence to the recovery of losses (unless cash and then usually there is no recovery)!:

U.S. Federal Trade Commission: **https://www.identitytheft.gov**
U.S. Dept. of Justice Elder Fraud Hotline: **https://www.justice.gov/stopelderfraud**
Federal Bureau of Investigation: **https://www.ic3.gov**
National Center for Victims of Crime, Financial Fraud Victim Recovery Checklist:
https://victimsofcrime.org/victim-recovery-checklist/

GENERAL WARNING SIGNS OF A SCAM

These usually involve some kind of verbal ruse over the phone from someone you do not know, however, it may be someone you do know or think you know, such as in cases of a romance-related or tie-in scams like the "Granny Scam." Note that legitimate persons from the agencies and organizations referenced below will never call you for official business reasons.

1) Person threatens to take some sort of immediate financial or legal action against you unless you provide payment immediately.

2) Person urges or demands that you take some kind of action immediately that will benefit them or an organization.

3) Person urges or demands that you provide a credit card number or checking account number to pay a late bill or fine.

4) Person claims they are with a local, federal or state agency (IRS, FBI, Social Security, Medicare, other law enforcement) or utility company, etc., and demands that you take some kind of action (usually make a payment with a credit card, gift card or checking account number and/or provide some other kind of personal or financial information) under threat of immediate punitive action against you, including warrants for your arrest.

5) Person call or says they are coming to your house to deliver some kind of prize/lottery/sweepstakes winnings or other gift(s). The other sign here is that they say they will need a small (initially) fee, paid in the form of a **gift card** (Green Dot, iTunes, etc.) to pay taxes, register your winnings with the FDIC, IRS, etc. If you legitimately win, the **only** paperwork you should be asked to fill out is a form the prize presenters are required to file with the IRS and state tax commission (and you should never do this online). You **never** have to pay a **fee** for winning a prize, only taxes (which are sometimes taken out **before** you receive your prize money) and **only** to the respective governmental agency **directly**. This ruse is common with Publishers Clearing House (PCH) prize scams and can become a very dangerous scam that can morph into a complete life takeover and drain you of all your assets.

6) **Any type of activity** that involves you paying any kind of fee, most often with a **gift card**, Green Dot card, iTunes card, Vanilla Visa, etc. Remember, gift cards are for gifts only, not for paying bills!! Or any transaction requiring payment in gold, silver, cryptocurrency, or any other type of "non-standard" form of payment or that requires you to go to an ATM or Western Union office to make the transaction.

7) Person you've met online and or may have a romantic interest in asks you to pick up and re-ship (transship) any type of package, goods, etc., to a third party or forward money to a third party via Western Union, MoneyGram, ACH or wire transfers, Zelle, Venmo, CashApp, etc., or asks you to send them money for a plane ticket to come see you, help pay for medical costs for a sick relative, or anything else that involves you moving money or goods for them or sending them money for any reason – this is common in romance scams and makes you a "money mule," which is an illegal activity. See the FBI's Money Mule Awareness page here[1].

8) Person calls you out of nowhere with a strange, but seemingly harmless question, then calls you back days or weeks later, for whatever reason, and starts to develop a friendship with you – chances are they are using a technique called "social engineering" to "cultivate the halo effect" and "groom" you for victimization of some kind. This can be a process that goes on for weeks, months or even years before the crime occurs. If you are a prolific user of social media, you are much more susceptible to this type of crime because you have given the criminals a significant amount of your personal information to work with. This is also known as an "affinity" crime and sometimes "pig butchering."

CRITICAL STEPS TO AVOIDING SCAMS

1) **DO NOT** conduct any kind of complicated business when you are physically or emotionally tired, stressed, distressed, or under the influence of any drugs (Rx or illegal) or alcohol that may cloud an otherwise clear thought process. Ask a trusted, knowledgeable friend or relative for help, if necessary.

2) **DO NOT** answer the phone unless you recognize the number or name. **Even then**, remember, Caller ID's [and now voices using Artificial Intelligence (AI)] can be spoofed to appear or sound like anyone from the President to your parents, spouse or child, financial institutions, law enforcement, etc., so be very careful. If in doubt, hang up, get the number yourself off a billing statement, official online website or account, local bank branch, back of credit card, or other trusted source and call them back.

3) **DO NOT** answer the door unless you know who it is. Get an easy-to-set up Blink[2] or other brand wi-fi enabled doorbell camera – $50 or less. Official credentials and uniforms can easily be mimicked by criminals. If someone shows up and claims to be with law enforcement and demands you open the door, call 911 to confirm that they have been dispatched to your location.

4) **DO NOT** let anyone, especially someone you don't know personally, for any reason, intimidate, scare or shame you into providing personal or financial information or payments or coerce you into engaging in questionable activities. (moving money, trans-shipping goods, etc. – See #7 in the previous section.)

5) **DO NOT** open text messages, e-mails, pop-up ads from unknown senders and if you do, **DO NOT** click on any links inside or call any phone numbers contained in them - doing so can install all kinds of malware on your computer or cell phone or put you in personal contact with the scammers. **Think before you click or call!**

[1] https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/money-mules
[2] https://blinkforhome.com/

6) **DO NOT** give anyone remote access to your computer unless **you initiate** contact and you are **absolutely certain** they are a legitimate computer repair service and not a scam. Pop-up warnings for virus infection/tech support on your computer are generally scams. Do an Internet search of their name and or toll-free number for scam reports.

7) **DO NOT** use (insert or swipe) a **debit** card in any point-of-sale terminal, gas pump, etc., where skimmers/shimmers may be present. *(In fact, consider getting rid of any **debit** cards – they can give criminals **direct access** to all the money in your bank account.)* Commercially, publicly available devices claiming to be able to detect the presence of skimmers/shimmers may not always detect all of them. Pay with cash, dedicated gas station credit card, other credit **(not debit)** card, limited amount gift card.

8) **DO NOT** store payment information (credit card numbers, bank account numbers, etc.), on websites that offer this as a convenience for making future purchases. **See #1 below.**

9) **DO NOT** send money, funds, anything of value, etc., in any form or via any method or give out personal information to someone you don't know.

10) **DO NOT** arrange to meet people you don't know. If you must, say for a legitimate transaction (purchase or sale) for goods, meet in a very public place and take a friend with you and let a 3rd party who will not be present know the full details of those activities and set a time for you to check in with them and establish and emergency code word/phrase.

11) **DO** add a "trusted contact" (not necessarily a joint owner) to your financial accounts in the event you become incapacitated or a victim of fraud. Make sure you know and trust this person very well!

12) **CRITICAL: DO** have a special family "code word or phrase" for emergencies so you know you are really speaking with an actual family member and not a scammer or AI impersonating someone. Do not e-mail, text or post anywhere online this code word/phrase.

13) **DO** use a Medicare Healthcare Journal and compare it to your EOB's (Explanation of Benefits) or MSN (Medicare Summary Notice) paper or online statements for fraudulent activity or billing errors. Be very wary of significantly delayed billing dates from what you have in your journal. **Note:** People on Medicare Advantage Plans and Medicare Part D receive EOB's and people on regular Medicare receive MSN's. In OK, order journals by calling the Medicare Assistance Program office at 800-763-2828. If you are in another state, just do an online search for "(your state's name) Medicare Assistance Program)"." You can also view your Medicare statements/charges with your online account at: https://www.medicare.gov

CRITICAL STEPS TO SECURING YOUR PERSONAL INFORMATION

1. **DO** use passwords/passphrases at least 12 characters long (combination of upper and lower case letters, numbers, symbols, spaces). Use a unique password for each account – no duplicates. Change passwords every 6 months. **DO** use a third party password/credential manager like Dashlane[3], BitWarden[4] (or others) on all your electronic devices to secure your information. Alternatively, here is info on constructing a paper password management system[5]. **DO NOT** use any of these 50 most common passwords[6].

2. **DO** enable 2-step login (aka 2 factor authentication, 2FA) protocols on **ALL** your online accounts where you have to enter your user ID and password to log in.

3. **DO** set up text alerts on all your banking and credit accounts so that you will receive an alert text or e-mail any time **any** transaction has occurred with those accounts. Immediately contact the fraud departments of those accounts if you did not initiate the transaction.

4. **DO** review your consumer credit reports[7] and ChexSystems[8] reports at least annually. Because of all the Covid-related fraud, the credit bureaus are still allowing you to view them for free on a weekly basis.

5. **DO** consider signing up for free credit monitoring services with Credit Karma[9] and Credit Sesame[10] **BEFORE** taking step 7.).

6. **DO** set up online accounts (before someone else does it for you) with: Social Security (includes Medicare)[11], eBenefits[12] (military & government benefit recipients), VA[13], USPS[14], USPS Informed Delivery[15] **BEFORE** taking step 7.).

7. **DO** consider a credit freeze or credit lock (they are different) with the Big 3 credit reporting agencies[16] and the NCTUE[17], even and especially for children. If you do, be sure to keep your login credentials in a very safe place!!! And do this **AFTER** steps 4.) thru 6.), otherwise you will have to go through the process of unlocking or unfreezing your accounts to sign up for some of them or get a special temporary passcode from the government agencies.

---

[3] https://www.dashlane.com/
[4] https://bitwarden.com/
[5] https://www.blackhillsinfosec.com/the-paper-password-manager/
[6] https://thriveweb.com.au/blog/50-most-common-passwords-2022
[7] https://www.annualcreditreport.com/index.action
[8] https://www.chexsystems.com/request-reports/consumer-disclosure
[9] https://www.creditkarma.com/
[10] https://www.creditsesame.com/
[11] https://www.ssa.gov/
[12] https://www.ebenefits.va.gov/ebenefits/homepage
[13] https://www.va.gov/
[14] https://www.usps.com/ *(Yes, it is **.com** in this case since the USPS is not an official government agency)*
[15] https://www.usps.com/manage/informed-delivery.htm
[16] https://www.annualcreditreport.com/index.action
[17] https://www.nctue.com/consumers

8. **DO** only use a Uniball Signo brand #207[18] anti-fraud gel ink pen to fill out checks and **ONLY** place outgoing mail in a drop box **inside** a U.S. Postal Service substation during business hours. Note that **not** all "gel" ink pens use the special anti-fraud ink; it must say so on the packaging. Also, hold the envelope up to a bright light - be sure the envelope has adequate security features to mask what is inside (like a check) and insert additional pieces of paper to mask the contents, if necessary. **Best practice:** Go "paperless," get your monthly bills via e-mail, pay them online and avoid writing **any** checks if at all possible – they are one of the most compromised methods of payments at this time because our mail system is compromised now. Go to your local bank branch and sign up for online banking. Pay bills with a credit card (**NOT** debit card) or use auto draft to your checking account to pay monthly bills. You should have a **dedicated credit card** for recurring payments that is never used/swiped in a Point-of-Sale terminal like the gas station or grocery store. Also, you should have at least 2 bank accounts – one where the majority of your money is housed (and that you do not give out the account number) and a smaller one where you only move enough money each month to cover your bills. **Ideally,** pay each bill manually (instead of auto-draft), monthly once you receive your e-bill – this avoids you having your account number information stored on someone else's server where it could be subject to data breaches. Some banking apps, security software suites and PayPal allow you create a unique (virtual), one-time-use credit card number (tied to your actual credit card number) to make payments, that way, the vendor, nor anyone else, ever sees your real credit card number. Pay your taxes electronically, as well.

9. **DO** run some sort of **paid**, not free, third-party full software security suite (firewall, anti-virus, anti-spam, anti-malware, anti-ransomware, etc., to protect against malicious websites, spam, malware, viruses, keyloggers, other system intrusions, etc.) If you use a computer this is absolutely a **critical** step you **must** take, **no exceptions!** Bitdefender Total Security and Norton 360 Deluxe consistently get the highest ratings from industry publications. Just do a search for "best software security suite" for other options. Also, be sure to have a knowledgeable person adjust the software's settings to ensure that you have the maximum protection enabled. There are many other steps you need to take to be cyber-secure, so for more computer safety tips, be sure to read my free 170+ page ***Identity Theft*** e-Book on the **Publications** page of my website[19].

10. **DO** backup your computers files regularly. You can use an external hard drive such as a Western Digital Passport[20] external hard drive, or cloud back-up service like Carbonite[21] or iDrive[22]. Just remember, external hard drives are still susceptible to the same damage, loss, failure, and theft as your computer.

11. **DO** check with your local county clerk or assessor to see if they offer some type of "lien alert system" to notify you about unexpected changes to your home's (or other real estate holding's) title(s) and or deed(s) and sign up for it. Yes, home theft is becoming a big problem.

[18] https://uniballco.com/collections/207
[19] https://www.magnusomnicorps.com/publications.html
[20] https://www.westerndigital.com/
[21] https://www.carbonite.com/
[22] https://www.idrive.com/

REMEMBER THESE WORDS OF WISDOM

1) If it sounds too good to be true, it probably is.
2) There is no free lunch.
3) If you didn't enter the contest, you can't win. (Foreign lotteries are illegal in U.S.)
4) When in doubt, check it out! (Do an Internet search for scam-related reports.)
5) Think before you click or call!

STAY UP-TO-DATE WITH ALL THE LATEST SCAMS & FRAUD & GET THE BEST SAFETY TIPS BY JOINING YOUR LOCAL COUNTY SHERIFF'S TRIAD GROUP (more info here)[23]!!! OPEN TO THE PUBLIC, FUN, FREE & NO COMMITMENTS. DO IT NOW!!!

For more information, get your free, 180+ page e-book

Special Report: Identity Theft, Financial Fraud & Cyber-Crime – Problems, Solutions and Mitigation Strategies ***at:***

https://www.magnusomnicorps.com/publications.html

BEST INTERNET RESOURCES TO KEEP ON TOP OF FRAUD AND SCAMS

I strongly suggest subscribing to the periodic newsletters (e-mails) and podcasts from the websites that offer them. These websites do not sell or otherwise share your contact information.

http://www.aarp.org/money/fraudwatchnetwork

https://www.bbb.org/scamtracker/us

http://www.fraudoftheday.com/

[23] http://www.magnusomnicorps.com/oklahoma-county-triad.html

http://www.krebsonsecurity.com

http://www.getsafeonline.org

https://www.consumer.ftc.gov

http://www.cyberguy.com

http://www.komando.com

http://www.clark.com

https://twit.tv/shows?shows_active=1

https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

https://www.upguard.com/blog/biggest-data-breaches

https://www.identityforce.com/blog/2023-data-breaches

https://www.identityforce.com/blog

https://www.consumeraffairs.com/finance/identity-theft-statistics.html

http://www.magnusomnicorps.com/publications.html