Revision 202201016

ID THEFT, FINANCIAL FRAUD & SCAM REMINDER TIP SHEET

CRITICAL STEPS TO AVOIDING SCAMS

1) **DO NOT** answer the phone unless you recognize the number or name. **Even then**, remember, Caller ID's can be spoofed to appear like anyone from the President to your parents, spouse or child, so be very careful. If in doubt, get the number yourself off a bill, official online website or account, or other trusted source and call them back.

2) **DO NOT** answer the door unless you know who it is.

3) **DO NOT** let anyone, 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.)

4) **DO NOT** open text messages, e-mails, pop-up ads from unknown senders and if you do, **DO NOT** click on any links inside them - doing so can install all kinds of malware on your computer or cell phone. **Think before you click!**

5) **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. Google search their name and or toll-free number for scam reports.

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.*

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, 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 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 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. You **never** have to pay a **fee** for winning a prize, only taxes and only to the respective governmental agency directly. Common with Publishers Clearing House (PCH) prize scams.

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!!

7) Person asks you to pick up and re-ship any type of package, goods, etc., to a third party or asks you to use Western Union, etc., to forward money (ACH transfers, etc.) to a third party. Common in romance and money mule scams.

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 or even months before the crime occurs. If you 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.

REMEMBER: These criminals are very sophisticated, both technologically and psychologically. Some have 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. 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!!! So, no matter who you are, your age, educational level or socio-economic status, these kinds of crimes affect everyone, so please, do not be afraid or ashamed to ask for help if you suspect you have been scammed or are being abused or exploited, financially or otherwise. Law enforcement recognizes that these are serious crimes and they sincerely want to help stop them.

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! (Google search for scam-related reports.)
5) Think before you click!

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)[1]!!! OPEN TO THE PUBLIC, FUN, FREE & NO COMMITMENTS. DO IT NOW!!!

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

For more information, get your free, 104-page

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/scams-fraud/fraud-watch-network

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

http://www.fraudoftheday.com/

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

https://www.identityforce.com/blog/2021-data-breaches

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

In addition to reporting any crimes to the police, go here immediately if you have been a victim – this website outlines everything you need to do to recover and protect yourself and your assets:

U.S. Federal Trade Commission-sponsored website:
https://www.identitytheft.gov