Invisible Victims…….Invisible Crimes

Assisting Older Victims of Transnational Technology Assisted Frauds/Scams

Debbie Deem, Retired FBI Victim Specialist, Los Angeles

'A Team' member (CA CEJC) Former FAST Coordinator, Ventura County

NAPSA Volunteer Facilitator for the monthly Scam Advice Forum

deemstrategies@gmail.com

https://ovc.ojp.gov/program/stop-elder-fraud/link-us

Additional Guidance/Sharing for Professionals

Join us on the monthly NAPSA Scam Forum, 4th Thursday of most months for professionals working with older/adults disabilities victims of international technology facilitated frauds/scams.

Share challenging situations, advice and suggestions from other direct services/supervisors, share successes, new resources, etc. (Scroll to purple section)

- https://www.napsa-now.org/financial-exploitation/
- Past forums and resource lists
  - https://www.napsa-now.org/blog/

Transnational Frauds

- Cyber-fraud crime is any activity that uses the internet to access, transmit, manipulate internet data for illegal purposes.
- Technology Facilitated Frauds/Scams- evolving nature of technology as one weapon of fraud

    - These crimes often involve many criminals operating in foreign countries but may pretend to be in the US.
        - Victims may believe they are only dealing with one person.
        - There are often money mule cells/gangs that operate in the US working for these groups, and often enlist victims to unknowingly assist as money mules/money movers.
        - Transnational organized crime rings are involved.

    - **This makes investigations/arrests/getting money back difficult or impossible.**

Fraud Fighter Crime Tip: Phone Security

- **FTC reports the phone was the 2nd highest way fraud criminals targeted victims in 2023**
- Only pick up the phone from numbers from those you know and trust (are in your phone directory)
- There are ‘anti scam’ call blockers you can get for your phones
  - Don’t trust caller ID
  - Let calls go to voice mail. This is screening your calls. Then you can choose whether to call back.
  - If it’s a government agency or bank, don’t call them on the number they provide- instead look for a past bill or statement, or careful search online and use that number to call.
  - Sign up for the FTC’s Do Not Call List
    - USPIS Screening phone calls handout.
    - https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts
    - https://www.fcc.gov/call-blocking

Will the “Do Not Call List” Stop All Telemarketing Calls?
NO
But Still Critical to Include ‘Let Calls Go To VM’ Warnings

- Register with FTC’s Do Not Call List at 888-382-1222 or www.donotcall.gov
- Will not stop criminals from calling pretending to be legitimate

Avoid Victim Blaming- Focus on Criminal's Wrongdoing

- We each may be susceptible to fraud- different frauds for different people/ages.
- Avoid victim blaming/shaming. Promote victim's self – esteem, resiliency.
  - Begin each conversation- "I'm so sorry this happened to you".
- It is the criminal that is at fault. It is also a major reason so many victims do not report these crimes to families and police.
  - Avoid victim blaming in words we use-
    - Money taken was not 'losses'- it was stolen, crime victims were not conned, didn't fall for it, not duped- they were manipulated, they were robbed.
    - Headlines revictimize- "Victim fell for romance or lottery scam"
  - These criminals are not con artists, con-men, scammers -they are fraud criminals or fraud predators.

How Are Victims of Transnational Frauds Found?

Report These Crimes To These Federal Agencies

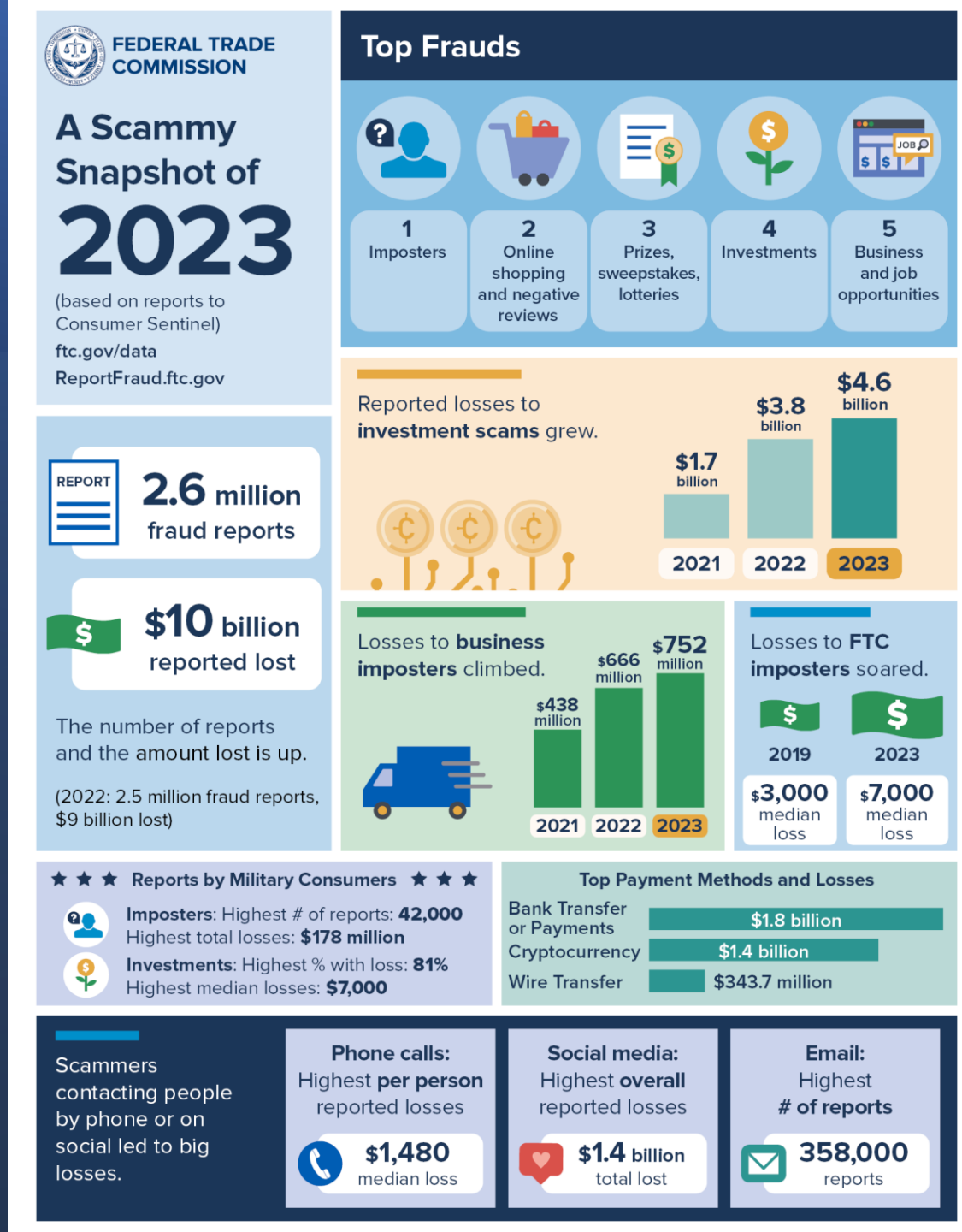
(in addition to police, APS)

WHY REPORT?

- Many are not aware of these government agencies for additional reporting
- FBI's RAT Team- report early/notify bank
- Also consider local Adult Protective Services & State Attorney General, Ombudsman.
- Keep all documentation, correspondence and receipts
  - Download or print a copy- can't retrieve it
- Think of them as a library of complaints that sworn police all over US can access

www.ic3.gov
Internet Crime Complaint Center (FBI)

www.ReportFraud.ftc.gov
Federal Trade Commission


FEDERAL TRADE COMMISSION
A Scammy Snapshot of 2023
(based on reports to Consumer Sentinel)
ftc.gov/data
ReportFraud.ftc.gov
REPORT
2.6 million fraud reports
$10 billion reported lost
The number of reports and the amount lost is up.
(2022: 2.5 million fraud reports, $9 billion lost)
Top Frauds
1 Imposters
2 Online shopping and negative reviews
3 Prizes, sweepstakes, lotteries
4 Investments
5 Business and job opportunities
Reported losses to investment scams grew.
$1.7 billion
$3.8 billion
$4.6 billion
2021
2022
2023
Losses to business imposters climbed.
$438 million
$666 million
$752 million
2021
2022
2023
Losses to FTC imposters soared.
2019
2023
$3,000 median loss
$7,000 median loss
Reports by Military Consumers
Imposters: Highest # of reports: 42,000
Highest total losses: $178 million
Investments: Highest % with loss: 81%
Highest median losses: $7,000
Top Payment Methods and Losses
Bank Transfer or Payments
$1.8 billion
Cryptocurrency
$1.4 billion
Wire Transfer
$343.7 million
Scammers contacting people by phone or on social led to big losses.
Phone calls: Highest per person reported losses
$1,480 median loss
Social media: Highest overall reported losses
$1.4 billion total lost
Email: Highest # of reports
358,000 reports

FBI 2022 Report on Victims Age 60 and Over

Over 82,000 older victims reported $3.1 Billion in money stolen

This was an 84% increase from amount stolen in 2021

Tech support/call center frauds- most common- 17,800 older victims with losses of $587 million

https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3ElderFraudReport.pdf

In 2022, over 800,000 complaints totaling $10.3 billion stolen- all ages

Investment fraud 4,500 older victims reported - just under $1 billion. Largest 'losses'of any age group, increased over 300% from 2021

Average $ amount stolen from older adults reporting was $35,101

Over 5,400 victims reported more than $100,000 stolen

How Criminals Obtain Information

Dark web purchases/trades

Data breaches

Call center leaks

Other- public records, mail, social media, surveys, contests, ‘sucker lists’, repeat victims, cold calling.

How Much Money Criminals Get From Stealing Data on the Dark Web

- Stolen online banking logins: $50
- Credit card details and associated information: between $17-$120
- Online banking login information: $65
- Hacked Facebook account: $45
- Cloned VISA with PIN: $20

- https://www.privacyaffairs.com/dark-web-price-index-2022/

- Stolen PayPal account details,
  - minimum $1000 balances: $20
- Hacked web and entertainment services, like Uber and Netflix: up to $40
- US Driver's License $150
- Email database dump for 10 million US email addresses? $120

Common Predator Tactics
Red Flag Warnings of Fraud

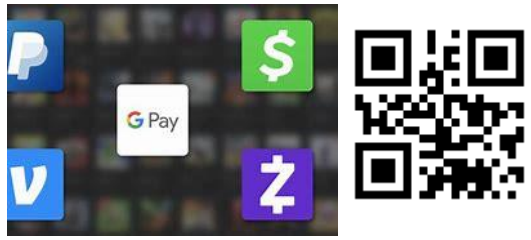
- An unexpected contact by a stranger or govt/business
- A request or demand for money or personal information or relationship
- Often demand urgency and/or secrecy
- A threat or enticing offer, attention/flattery- leading to heightened emotional state (panic/fear, excitement)
  - So victims are not rationally thinking- Instead, stop, take time to review/research before acting.
- Demand for a particular type of payment
- May involve financial grooming- small amounts of money leading to theft of larger amounts. Don't stop until all financial assets are stolen- and more.

Payment Methods Used by Fraud Criminals- How They Collect Their Money

Wiring Money

Reloadable debit/gift card

Peer to Peer (P2P) QR Codes



Cash

Fake Checks/Overpayment

Purchasing/Reshipping equipment

Cybercurrencies/BTM's

33,000 in US

Money Mules

Find a Crypto-ATM Near You https://coinatmradar.com/

Fraud Fighter Crime Tip

Have a TCP on all financial accounts

- Share account information and real time transaction notice on your accounts with someone you trust.
- Consider a trusted contact person (TCP) or emergency contact if you don’t have the person above. They will not have access to your account information.

There really is a fraud for everyone

Common types of technology facilitated frauds/scams

Some of which target older adults

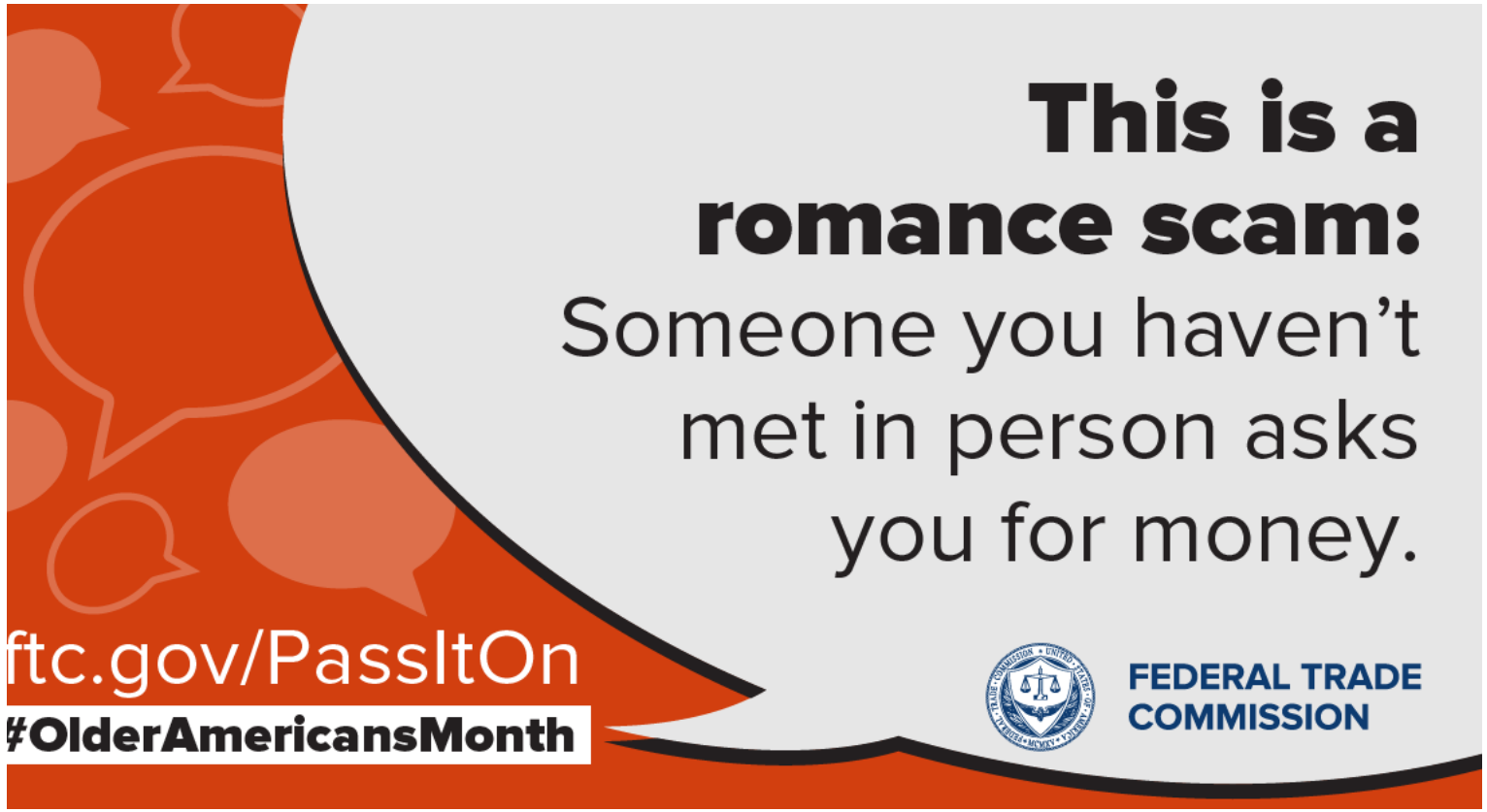
AND NOW- AI (Artificial Intelligence will impact all of these.)

Lottery and Sweepstakes Fraud	Romance Imposter Fraud	Tech Support/Customer Service/Computer Repair
Government and Business Imposter Fraud	Family Emergency Fraud	Identity Theft
Crypto Currency Fraud • Payment method and investment fraud	Used as Money Mule/Money Mover	Online Shopping Fraud

Additional Common Frauds

Job ads
Phishing/smishing – fake invoices, package delivery
Identity Theft
Extortion/sextortion
Robocalls
Nonpayment/Non-Delivery, Fraudulent Products
Health care fraud
Foreclosure rescue frauds
Charity/disaster fraud
Vacation/time shares
Payment in any fraud by Gift cards or Crypto-currency

Overview of Current & Trending Transnational Frauds



Online Romance Imposter Frauds

Romance Imposter Predator Tactics

Targeting and Recruitment-

- Find a lonely person
- Information gathering, mirroring of experiences, dreams
- Perpetrators use chat rooms, social media, dating sites to choose potential victims
- Create Ideal persona to 'present'

Cyber seduction- make them feel wanted

Grooming/In control of the relationship/ 'love bombing'

Isolation from 'real connections, events and people'

May pose as celebrity

Execution of the financial requests, test and follow up requests for money/involvement 3rd party for money dealings

Need to sacrifice with financial support so we can be together.

Repeat- until victim broke and in debt

Engage the victim in crime- as money mule/mover

- Financial Transactions
- Traveling- use as money or drug mule

Coercion/Threats/Sextortion

Victim may steal from family/work, borrowing money

Once identified – may 'ghost' the victim- but may reappear as new potential suitor or later apologizes to 're-hook' victim, or show real self- in love really

Victim Tells Her Story

https://www.youtube.com/watch?v=108UWM1jsF8

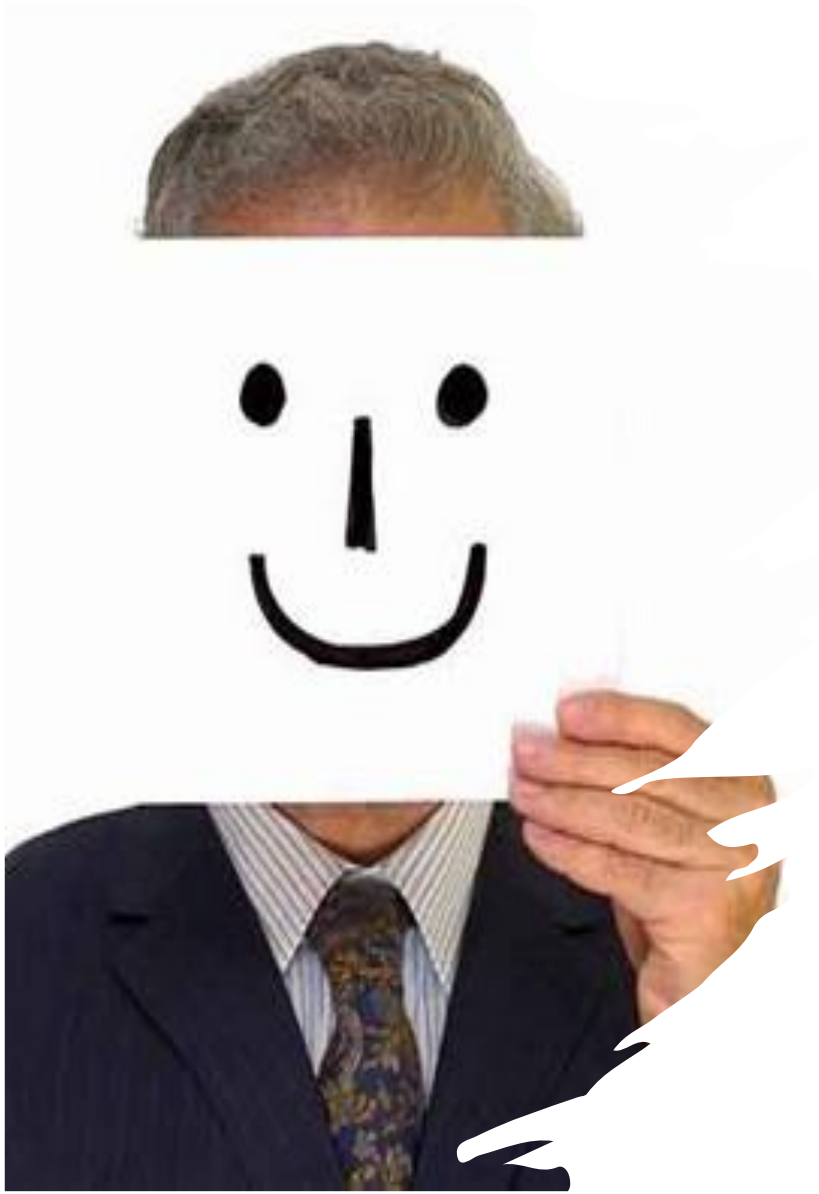
Victim reported $2 million stolen from her in this case

Fraud Fighter Crime Tip:

End the 'Relationship Immediately & Report

- Once you send money you will not get it back, no matter what they promise or you try to negotiate. You may end up having even more stolen, especially if you gave them bank account information.
- Stop communication with the fraud criminal. Don't respond to any requests/promises/threats.
- Secure your accounts. Freeze credit. Notify your financial institutions of any compromised accounts- close and change.
- Assume computer/cell may have malware installed.
- Report the crime- practice financial self defense-lock down your accounts and deny the criminal access.
- Be prepared for future contact. Find support and activities to help you through this.
- There are free support groups online or by phone to help.

Government & Other Imposter Fraud/Call Center Fraud



- **Caller says from IRS, Social Security, other govt or business agency - may show on caller ID**
- May give badge number and have last 4 digits of SS#
- You are told you owe money, SS # was suspended
  - Pay now or you will be arrested
  - Put money on gift card, crypto ATM/QR code or wire it
  - Insist you stay on cell phone until payment made
- If you pay, you will find out it wasn't the IRS, Social Security (bank, computer company, jury duty, utility)
- Grandparent/family emergency frauds as well- now using AI.
- www.fightcybercrime.org

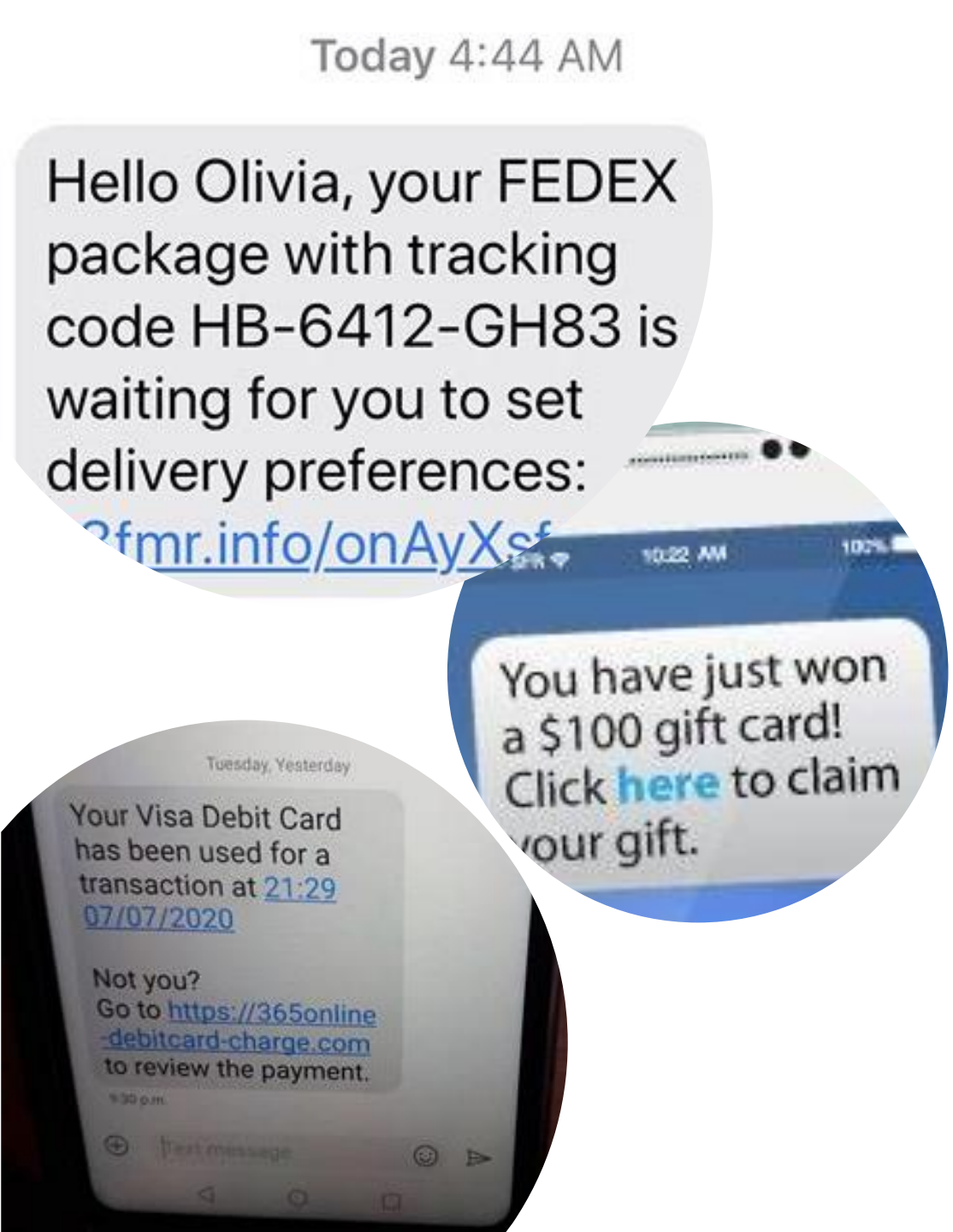
Fraud Fighter Crime Tip:

Put a Freeze On Your Credit

- For tips on how to do-
  - Contact Identity Theft Resource Center www.idtheftcenter.org or 1-888-400-5530
  - Contact FTC's www.identitytheft.gov

- To receive free copies of your 3 credit reports you can also request them at www.annualcreditreport.com

- Contact the national credit bureaus to request fraud alerts, security freezes.
  - **Equifax** Equifax.com/personal/credit-report-services 800-685-1111
  - **Experian** Experian.com/help 888-EXPERIAN (888-397-3742)
  - **Transunion** TransUnion.com/credit-help 888-909-8872



Have you Been 'Smished'?

- Victims may also get smishing emails or texts saying a bank, Netflix, Amazon, FedEx or other account saying it is closed, or package to be delivered- want you to click on link to renew service or schedule a package.

- **Smishing** is a form of phishing that involves a deceptive text message or phone number that intends to lure the recipient into providing personal or financial information or money.
  - Criminals seek account usernames and passwords, Social Security numbers, DOB, credit and debit card numbers, PINS and other sensitive info
  - Forward the texts to '7726'
  - "Haveibeenpwned.com- emails, phone numbers found in some data breeches

- DON'T Do It. Treat your personal information like cash.
- https://www.consumer.ftc.gov/articles/how-recognize-and-report-spam-text-messages

Lottery and Sweepstake Fraud: There Is No Grand Prize- EVER


PUBLISHERS CLEARING HOUSE

DEAR

The team at Publishers Clearing House is pleased to officially announce you, as a second Place winner in the 100 Million Dollars Super Cash Giveaway Promotion sponsored by Readers Digest, Mega Millions and Multi-State Lottery Association.

The total amount to be claimed for your win is Five Hundred Fifty Thousand us ($550,000) Congratulations!

The Publishers Clearing House has made all necessary arrangements in order for you to receive your prize. Enclosed in this letter is a check of $7,800.00 which is part of your winning.

Please contact your Claim Manager without any delay BEFORE depositing this check at your financial institution and for further information on this prize.

- Usually begins through 'bait' solicitations:
  - Mailings, email, social media, text or phone calls
  - Often impersonate legitimate companies such as Mega-millions or Publishers Clearinghouse
- Victims are required to send money in advance for taxes, fees – not allowed under federal law.
  - Participation in foreign lotteries against the law "876"
  - You never have to pay taxes or other fees in advance of winning
  - Victims can be lured and 'ensnared' for years
- Amounts seem small at first– reloaded-escalate
  - Will demand life savings, encourage borrowing money
  - Frequently involves counterfeit checks and being used as a money mover/mule
  - PCH Fraud reporting: 1-800-392-4190

Actual Call From A Lottery Fraud Criminal

https://www.youtube.com/watch?v=wFkqUgDYo7M

He stole over $300,000

Sentenced to almost 6 years.

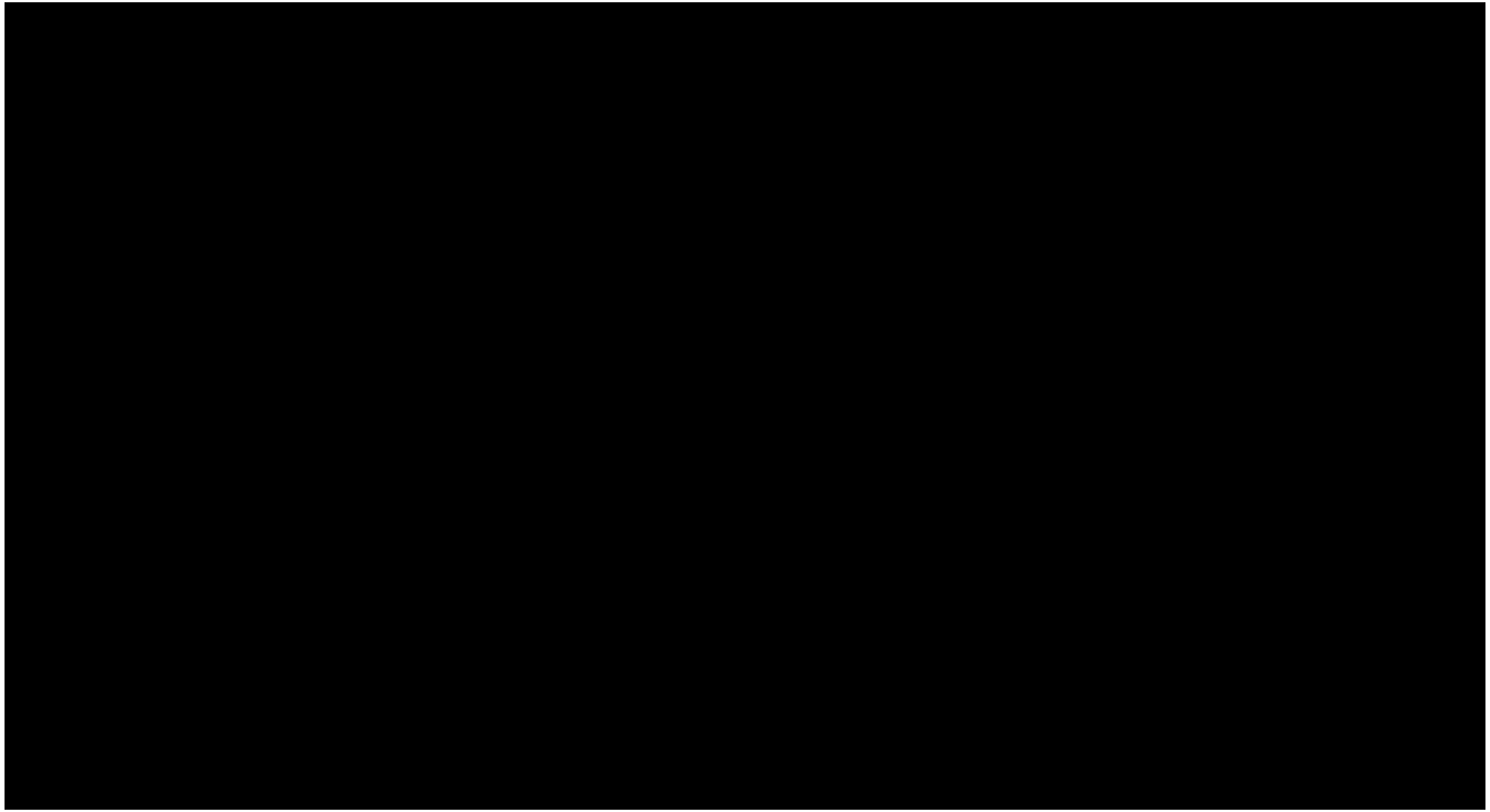
Tech Support Crimes

- Older adults are the most vulnerable - this is the online fraud crime most likely to succeed
  - Reports 5 times higher than other age groups (FTC)
- Several ways that this crime is initiated…….
  - Phone call impersonation
  - Popup- computer in danger
  - Find fake tech company online
  - Recovery of money from security program
  - May lead to bank security imposter frauds- and other crimes
    - Authorized Push Payment (hypnofraud)
    - Phantom Hacking (FBI term)

- Guidance for victims:
  - https://staysafeonline.org/online-safety-privacy-basics/how-to-tell-if-your-computer-has-a-virus-what-to-do-about-it/
  - https://www.aarp.org/money/scams-fraud/info-2019/tech-support.html
  - FTC guidance on tech support https://www.consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams
  - IC3.gov guidance can be found at https://www.ic3.gov/media/2018/180328.aspx
  - https://fightcybercrime.org/technical-support-imposter-scams/

“Phyllis” Tech Support Fraud

https://www.youtube.com/watch?v=ar2MOvn2aDc&t=2s



Trends/Future Technology? Are We Prepared?

- Money mules/movers and use of couriers to pick up money from a victims' home.
- Sextortion/extortion/ransom
- Phantom Hacking/Authorized Push Payment Fraud (APP) bank security impersonators
  - Banks distinguish between a 'scam' and a 'fraud'- victims not reimbursed- since 'authorized' the transaction even if bank or other impersonator.
- Financial Grooming - Crypto-investment fraud "pig butchering"
- AI Deep fake images (face swaps) and deep fake voice cloning
  - Celebrity imposters, family emergency/grandparent fraud, romance, lottery
    - Chat GPT future? https://chat.openai.com/auth/login
    - https://www.howtogeek.com/879206/how-to-tell-chatgpt-scams-apart-from-the-real-thing/
  - Senate Subcommittee on Aging- AI – Emerging Threat re Scams- brochure
    - https://www.aging.senate.gov/press-releases/casey-holds-hearing-on-role-of-artificial-intelligence-in-frauds-and-scams

Phantom Hacking

https://www.youtube.com/watch?v=Mif6VcYlzms

Fraud Fighter Crime Tip: Bank Imposter Frauds

- **Gift cards, crypto payments and wiring money are the most common payment methods demanded by criminals.**

- **A Scam vs. A Fraud- Important Distinctions banks may use if you are defrauded.**

Most banks interpret federal law in that that if you authorize a transaction' even though it's a criminal posing as your bank security or fraud investigator/manager, you will likely be held responsible and not reimbursed.

Family Emergency Frauds

Bob Sullivan- cloned AI voice

https://www.aarp.org/podcasts/the-perfect-scam/info-2023/criminals-using-ai-voice-cloning.html

Family Emergency/Grandparent Frauds/Scams

- Often a grandchild- who says in deep trouble. Victim recognizes voice — he/she wrecked the car and landed in jail or a hospital.
  - Will have 3rd party do real 'negotiating'. Need victims' help by sending money.
- Fraud predators now can use voice cloning by using AI to clone the voice of a loved one.
- All they need is a short audio clip of your family member's voice — such as from content posted online — and a voice-cloning program.
  - When the scammer calls you, they will sound just like your loved one.

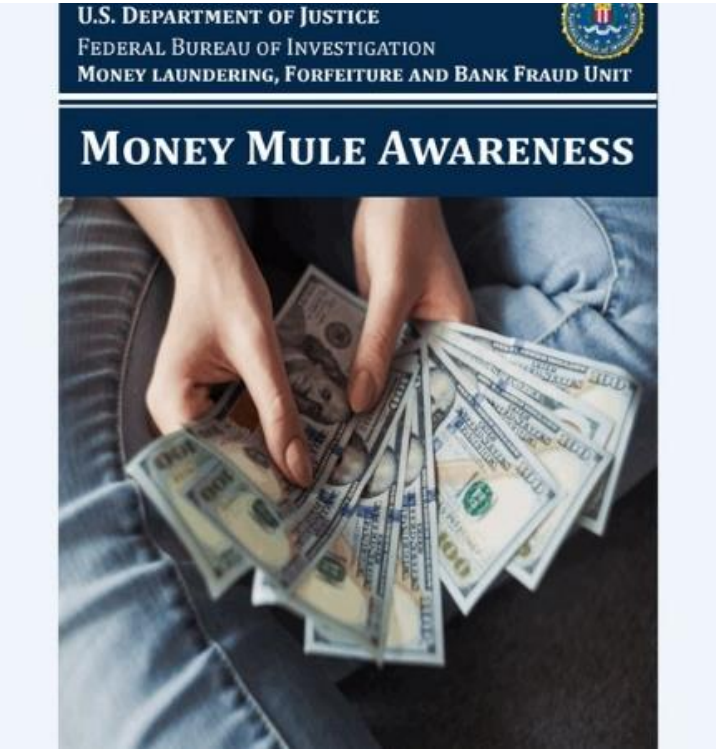
- Don't trust the voice. Experts suggest having a 'family safety code'
  - Scammer will try to keep you on the phone until transaction complete (and may repeat demands)
  - Call the person who supposedly contacted you and verify the story. Use their phone number and if you can't reach them, try to get in touch with them through family members or their friends.
  - May include 'couriers' to pick up the money at your home.

Signs of a Cryptocurrency Fraud

- **Investment (usually associated with relationship/romance imposters)**
  - A so-called “investment manager” contacts you out of the blue. They promise to grow your money — but only if you buy cryptocurrency and transfer it into their online account.
    - The investment website they steer you to is really fake, and so are their promises.
    - If you log in to your “investment account,” you won’t be able to withdraw your money, or only if you pay high fees
  - A scammer pretends to be a celebrity who can multiply any cryptocurrency you send them
  - An online “love interest” wants you to send money or cryptocurrency to help you invest
  - Scammers guarantee that you’ll make money or promise big payouts with guaranteed returns
  - Scammers promise free money if you send them money first
  - Scammers make big claims and guarantees without details or explanations
- **Payment Fraud**
  - Only scammers demand payment in a cryptocurrency (using local ‘ATM’s, often for lottery, romance and tech support, IRS and Social Security Imposters)

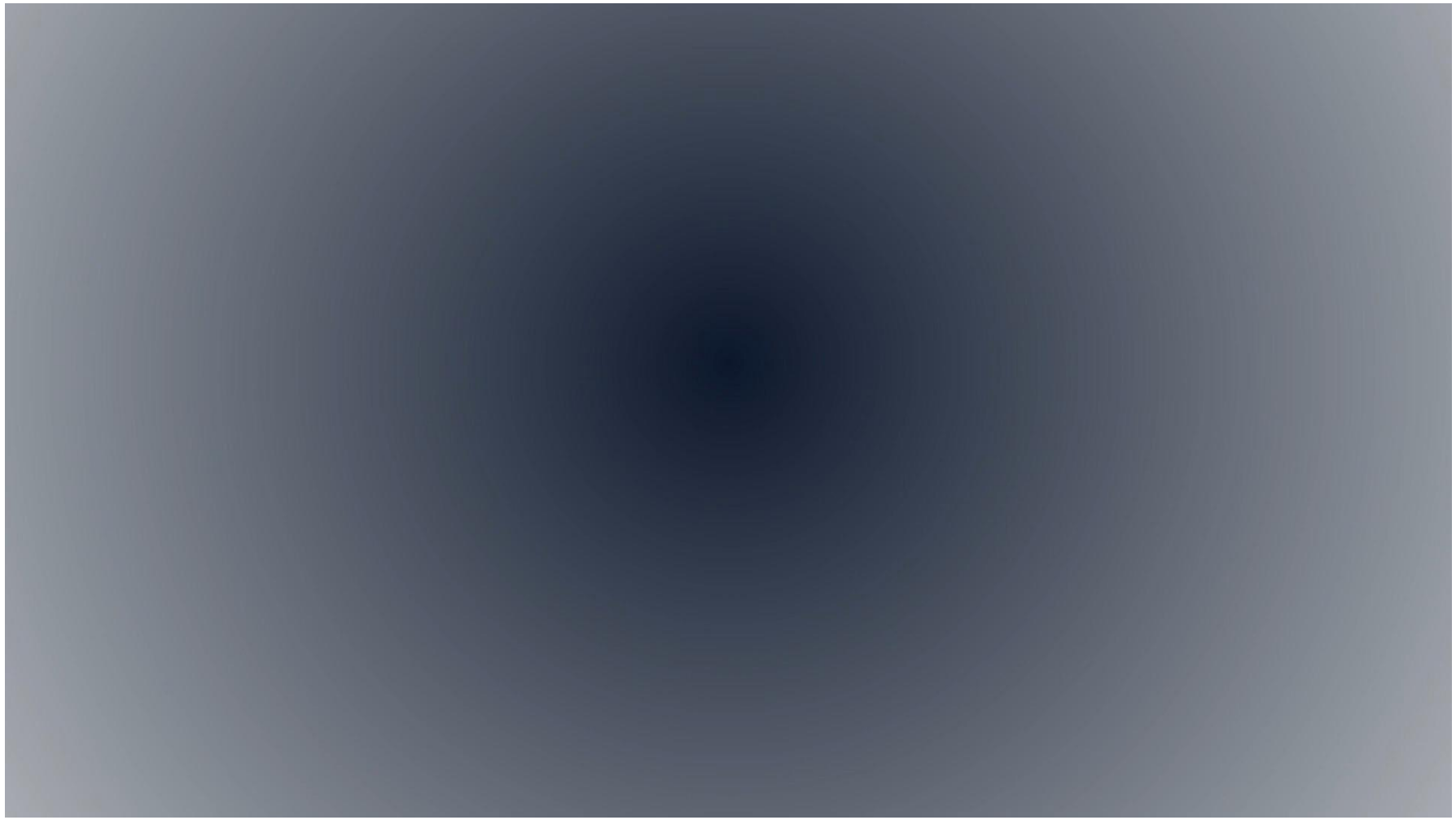
Victims Are Often Recruited To Be Money Mules/Movers

- A money mule is recruited and groomed by scam predators to serve as an intermediary to accept and further transfer stolen funds, property or drugs
  - Mules may or may not be aware they are being used
    - Witting or unwitting
  - Their function is to transfer fraudulently gained money to insulate fraudsters, making it difficult to identify the criminal.
    - Victim may be asked to open a new bank account and forward money to others.
    - Accept and forward packages.
  - They are prosecuted in US both locally and federally
  - It is money laundering



USPIS Warning on Money Mules/Movers

https://www.uspis.gov/news/scam-article/money-mule



Don’t Forget Basic Cyber Fraud Safety Planning

- Help in mastery/proficiency in tech equipment
  - Assess- victims may not know how to block calls, access voice mail, identify spam email, cut/paste, recognize phishing or how to update computer?
- Multi Factor Authentication MFA
  - Protecting account with something you ‘know’ (password/secret questions) and something you ‘have’- (cell phone one-time pass key) or ‘are’ (fingerprint)
- Mindful re: online profile (don’t include birthday year, widowed, divorced, age)
- Don’t the same password for email and other websites- use strong passwords
- Keep the systems and all applications updated

  Use privacy settings on social media- don’t ‘friend’ strangers- keep personal information off (marital status)
- Keep dating local- if can’t meet soon, move on. Don’t go off dating platforms quickly
- Investments- use licensed companies only.
- **Can they afford to have computer cleaned? OPTIONS?????**

- Who can victims contact if concern about possible cyber crime or computer issue?
  - Libraries and senior centers offering ‘tech’ support classes
  - https://stopthinkconnect.org/
  - www.Cyberseniors.org
  - www.fightcybercrime.org

https://ovc.ojp.gov/program/stop-elder-fraud/link-us

Free Facilitated Online Peer Support Groups

- Cybercrime Support Network (for romance imposter crimes) www.fightcybercrime/peer support
- Giveanhour.org Support group for Fraud Victims
- AARP ReST support groups (for victims and family members of all fraud crimes www.aarp.org/fraudsupport

Connections = Relationships= Hope

- If scammed, how are you helping them (and families) to identify and replace the fraud behavior/relationships with?
- “No matter how old we are we need a purpose.. A reason to get up in the morning”
- Recognize risk of re-victimization (recovery and new scams) and poly-victimization
- Don’t give up on them- took weeks/months to get into it, may take time to ‘leave’ and grieve the perceived relationship (similar to domestic violence), or dealing with dementia and need access to advocate or ‘coach” on daily/weekly basis with check ins.

Connecting With Others Online SAFELY

Online classes and meeting groups may help &'friendship' lines or services that 'check in'

- Cyberseniors: Connecting Generations https://cyberseniors.org/
  - https://www.youtube.com/user/cyberseniorscorner/videos
  - (past presentations on learning digital skills)
  - Provides free 1 on 1 appointment to learn how to use 'technology'
- GetSetUp https://www.getsetup.io Offers over 3,000 free classes
- AARP's Senior Planet https://seniorplanet.org/welcome/
- Deep Cover Learn to spot frauds online
  - https://www.buffalo.edu/ubnow/stories/2024/01/deepcover.html
- Covia.org https://covia.org/services/well-connected/
- University Without Walls https://www.dorotusa.org/our-programs/at-home/university-without-walls
- Foundation For Art and Healing- the Unlonely Project https://artandhealing.org/aging/
- Osher Lifelong Learning Institute- through local universities (CA State, Channel Islands)
- Local programs perhaps through senior centers, community colleges, libraries/local, state warmlines
- Virtual Memory Cafes for those with dementia to connect with each other- https://www.dementiamentors.org
- Victims with intellectual disabilities?
  - https://specialbridge.com and https://myspecialmatch.com

Additional Help And Support

- Link on website and have fliers made with information on these govt. websites.
  - **National Elder Fraud Hotline** at 1-833-372-8311 (camera ready to link to website)
  - Include links to ic3.gov and FTC reporting sites as well as www.identitytheft.gov

- FINRA's Senior Investment Helpline 1-844-574-3577
  - FINRA Broker Check to verify person/firm is registered to sell securities, offer investment advice or both https://brokercheck.finra.org/

- AARP Fraud Watch Network 1-877-908-3360 https://www.aarp.org/money/scams-fraud/helpline.html
  - Fraud support specialists provide information on what to do if defrauded/concern someone is contacting you to defraud you.

- Identity Theft Resource Center- www.idtheftcenter 1-888-400-5530
  - Identity Theft and the Deceased- guide and other useful tips/phone/text help (freezing credit)

- Cybercrime Support Network
  - Action plans, romance imposter fraud 10 week support group, cyber safety tips to lock down your technology www.fightcybercrime.org and https://fightcybercrime.org/programs/peer-support/

- Federal Trade Commission- information available in various languages
  - https://consumer.ftc.gov/consumer-alerts/2024/01/ncpw-speak-against-scams-your-language

- National Suicide Prevention Hotline Call or text 988

Free Informational Guides Useful to Customers
Download or Bulk Order - Consumer Financial Protection Bureau

Planning for Diminished Capacity and Illness Guide	https://files.consumerfinance.gov/f/documents/cfpb_planning-for-diminished-capacity-and-illness_consumer-advisory-bulletin.pdf
Considering a Financial Caregiver: Know Your Options	https://files.consumerfinance.gov/f/documents/cfpb_considering-a-financial-caregiver-know-your-options_guide_2021-05.pdf
**Choosing a Trusted Contact Person Can Help You Protect Your Money	https://files.consumerfinance.gov/f/documents/cfpb_trusted-contacts-consumers_2021-11.pdf
Guide to Managing Someone Else's Money:	Power of Attorney Govt. fiduciary Trustee Court appointed guardian •https://www.consumerfinance.gov/consumer-tools/managing-someone-elses-money/

Consumer Financial Protection Bureau Information Regarding Long Term Care Facilities

- Reporting Elder Financial Abuse Help for family and friends of people living in nursing homes and assisted living communities
  - https://pueblo.gpo.gov/CFPBPubs/pdfs/CFPB524.pdf

- Preventing Elder Financial Abuse: Help for family and friends of people living in nursing homes and assisted living communities
  - https://pueblo.gpo.gov/CFPBPubs/pdfs/CFPB522.pdf

- Preventing Elder Financial Abuse Guide for nursing homes and assisted living communities
  - https://pueblo.gpo.gov/CFPBPubs/pdfs/CFPB108.pdf

- Know Your Rights- Caretakers and Nursing Home Debts
  - https://www.consumerfinance.gov/consumer-tools/educator-tools/resources-for-older-adults/know-your-rights-caregivers-and-nursing-home-debt/

Trainings For the Public on Transnational Frauds

- FTC's Pass It On Campaign https://consumer.ftc.gov/features/pass-it-on
  - Bulk orders/download https://www.bulkorder.ftc.gov/

- FDIC and CFPB Money Smart For Older Adults https://www.consumerfinance.gov/about-us/newsroom/cfpb-and-fdic-release-enhanced-version-money-smart-for-older-adults/
  - Download and bulk orders https://www.consumerfinance.gov/consumer-tools/educator-tools/resources-for-older-adults/money-smart-for-older-adults/

- National Council on Aging Good resource on scams and frauds
  - https://www.ncoa.org/article/avoiding-scams-savvy-saving-seniors-financial-education

Thank You

Questions?

Buying a Product Online?

- **Study the Seller's Website** Is the price for the product too good to be true, compared to similar items you've seen?
- **Is the website secure?** Look for the padlock symbol in the address bar of your web browser when you visit a brand's website, along with https:// at the front of the web address. It means the website uses encryption to protect your data as it crosses the internet. It does not mean the website itself is legitimate or safe.
- **Does the brand offer any contact methods, like a phone number, address or email address?** These can be faked, but the absence of any contact information at all should send off alarm bells. What is return policy? Was product made in US (vs shipped from)?
- **How thorough is the website?** Look for privacy policy and terms and conditions pages, and an "about us" section. "Is the information sparse, in poorly written language, looks like it belongs to a different kind of company or even doesn't exist?"
- **2. Look for Authorized Resellers and trusted seller websites** Verify whether you're buying from a reseller or the company that makes the product.
- **3. Research Beyond the Storefront** Seek out reviews elsewhere. Do an online search for "brand x + reviews" Search "brand x + scam" or "brand x + fraud" Check reviews on bbb.org site
- **4. Use a Protected Payment Method** by using a credit card or a payment platform like PayPal. Credit cards typically offer full protection for the amount you spent in the event of fraud, but your debit card may not.
- Report to your credit card/other payment means, BBB and the FTC.
- https://www.forbes.com/advisor/personal-finance/online-shopping-scams/

And Finally….Ask One More Question…..

- “Do you have enough money to pay your rent or mortgage this month, or to buy food, or pay utilities”?

“We All Need A Reason To Get Up In The Morning” www.cyberseniors.org Connecting Generations

https://www.youtube.com/watch?v=bemDf6wuHJ0

Additional Support

- Local police and local APS
- National Elder Fraud Hotline 1-833-372-8311
- Consumer Financial Protection Bureau https://www.consumerfinance.gov/
- www.fightcybercrime.org Online help for cybercrime victims including action steps to do and where to report
- Identity Theft Resources
  - Identity Theft Resource Center www.idtheftcenter.org 1-888-400-5530
  - Information on credit freezes also available at https://www.consumer.ftc.gov/articles/what-know-about-credit-freezes-and-fraud-alerts
  - www.annualcreditreport.com (request free credit reports)
  - FTC Identity theft info- www.identitytheft.gov
- Report spam text messages information https://www.consumer.ftc.gov/articles/how-recognize-and-report-spam-text-messages
  - Copy the message and forward it to 7726 (SPAM)
- Cyber safety tips https://staysafeonline.org/stay-safe-online/
- AARP Fraudwatch Network and Hotline- 877-908-3360 https://www.aarp.org/money/scams-fraud/about-fraud-watch-network/
- National Suicide Prevention Helpline -800-273-8255 (TALK)
- Crisistextline.org Text **HOME** to 741741 from anywhere in the United States, anytime.