



Fraud Watch Network

Tech Talk – Medicare and Social Security Fraud

Overview

Fraud Watch Network

Watchdog Alerts, Tips & Resources, Free for Everyone



En español | The AARP Fraud Watch Network gives you access to information about how to protect yourself and your family. Non-members and members alike can get our Watchdog Alerts, stay up on con artists' latest tricks, and find out what to do if you've been victimized. It's free for everyone because AARP is committed to safeguarding Americans' financial futures.



AARP Shred Fest
Shred for free in your community. Find out where and when to participate

Text | Email | 57 | Share | Tweet | Like | 2.3K

GET SCAM ALERTS



Don't Pay for Your 'Missing' Money
April 29, 2016 7:20 PM

10 Tips to Avoid Rental Scams
April 22, 2016 12:00 AM

[See More Posts >](#)

MOST POPULAR

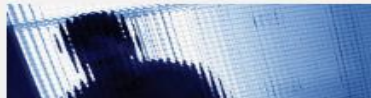


GET HELP AND RESOURCES



- Fraud Watch Helpline: 877-908-3360
- Who to Contact (PDF)
- Watchdog Alert Handbook (PDF)
- Protect Yourself from Holiday Scammers

MEET THE CON ARTIST



SOCIAL MEDIA

Connect with us on Facebook

#fraudwatch

AARP Colorado @AARPCO

Yes, you may be eligible for "unclaimed funds," but you don't need to pay to find them. [#fraudwatch](http://spr.ly/0019BW5Df)



Don't Pay for Your 'Missing' Money
You may be entitled to a piece of the ... blog.aarp.org

58m

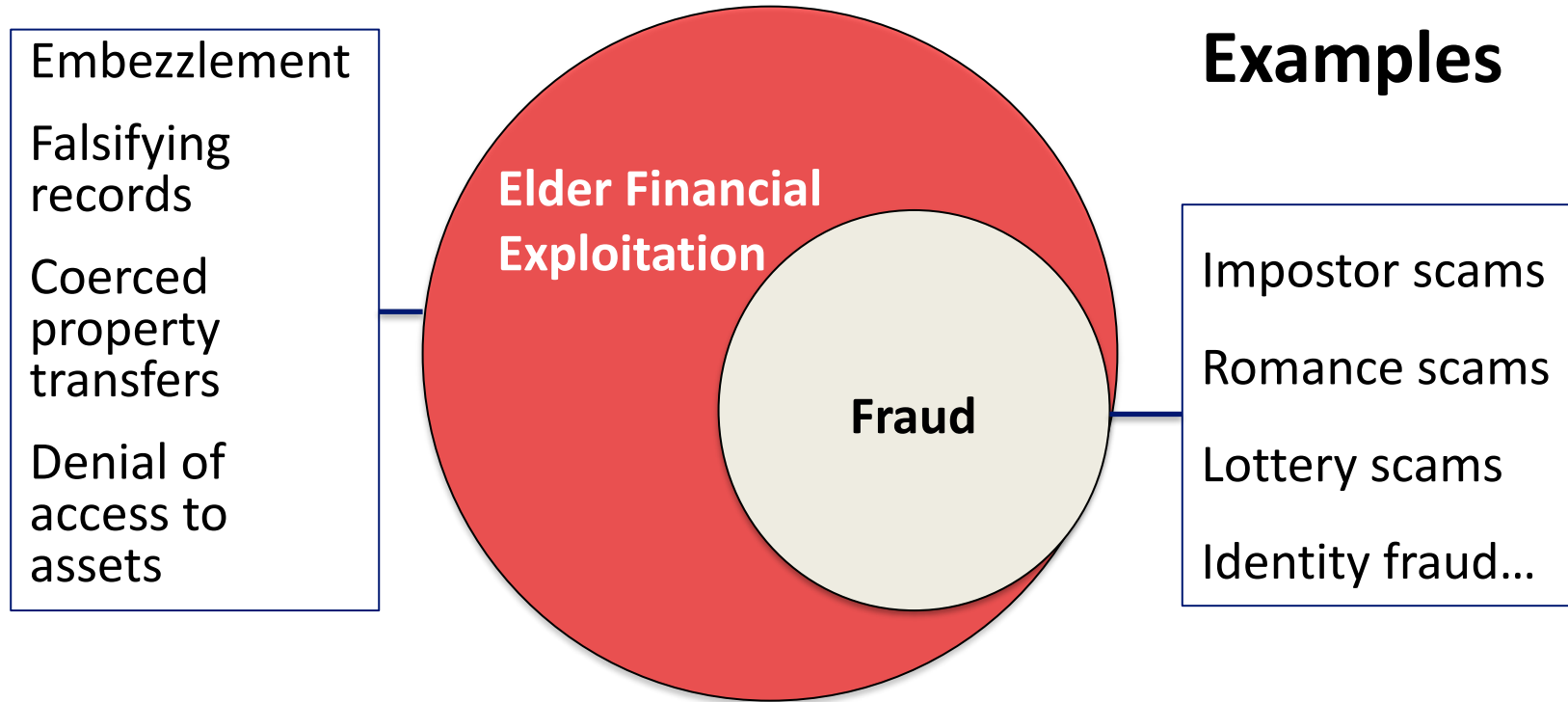
Rose Hobson Retweeted

AARP Maryland

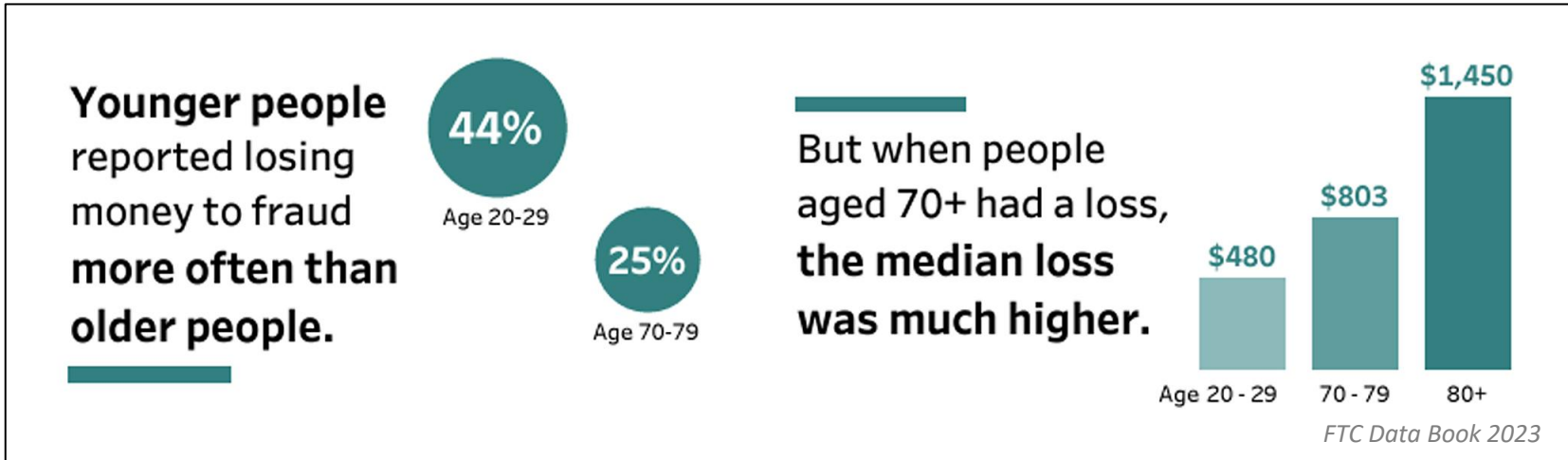
Agenda

- ❖ Overview
- ❖ Identity Theft – general
- ❖ Identity Theft – online
- ❖ Identity Theft – medical
- ❖ Prevention Strategies
- ❖ Resources

Fraud vs. Elder Financial Exploitation



Fraud & Older Adults



Younger people lose money to fraud more often.

Older people lose so much more.



Identity Theft - general

Identity Theft - general

DEFINITION



When someone steals your personal information (name, SS number & bank account information), and uses it to commit fraud or other crimes.

...opening credit accounts in your name, draining your bank accounts, applying for government benefits in your name; filing bogus tax returns...

Identity Theft - general

VULNERABILITY AND IMPACT



Leaving wallets, phones, laptops in our cars ... mail in an unlocked mailbox

Fraudulent purchases, locked out of online access to accounts, credit reports, affected credit scores and ability to get loans.



Identity Theft - general

EQUIFAX BREACH (AND OTHERS)

➤ Hackers may have stolen financial & consumer data on at least 143 million customers in the U.S. (birth dates, SS numbers, driver's license numbers, and address

- ✓ Visit equifaxsecurity2017.com (866-447-7559), find out, and sign up.
- ✓ Check credit report also with [TransUnion](#) and [Experian](#).
- ✓ Place credit freeze with all three companies (small fee).
- ✓ Add a [fraud alert](#) to your credit report.
- ✓ Monitor [credit card](#) and bank statements



Identity Theft - general

TIPS: low and high tech

- Have a locking mailbox
- Don't leave personal information in car
- Shred everything
- Check and monitor credit reports
- Establish online access to your accounts and monitor often
- Use caution using public Wi-Fi
- Use sophisticated passwords



Identity Theft – online

Impostor Scams: the Impostors

Government

- Social Security Administration
- IRS
- Medicare
- FTC
- U.S. Postal Service

Business

- Amazon
- Utility companies
- FedEx/UPS
- Norton
- Microsoft

What to Know

- The government and businesses do not contact you out of the blue about a “problem”
- Concerned? Contact the entity at a trusted phone number
- Make no payments, share no sensitive info

Identity Theft - online

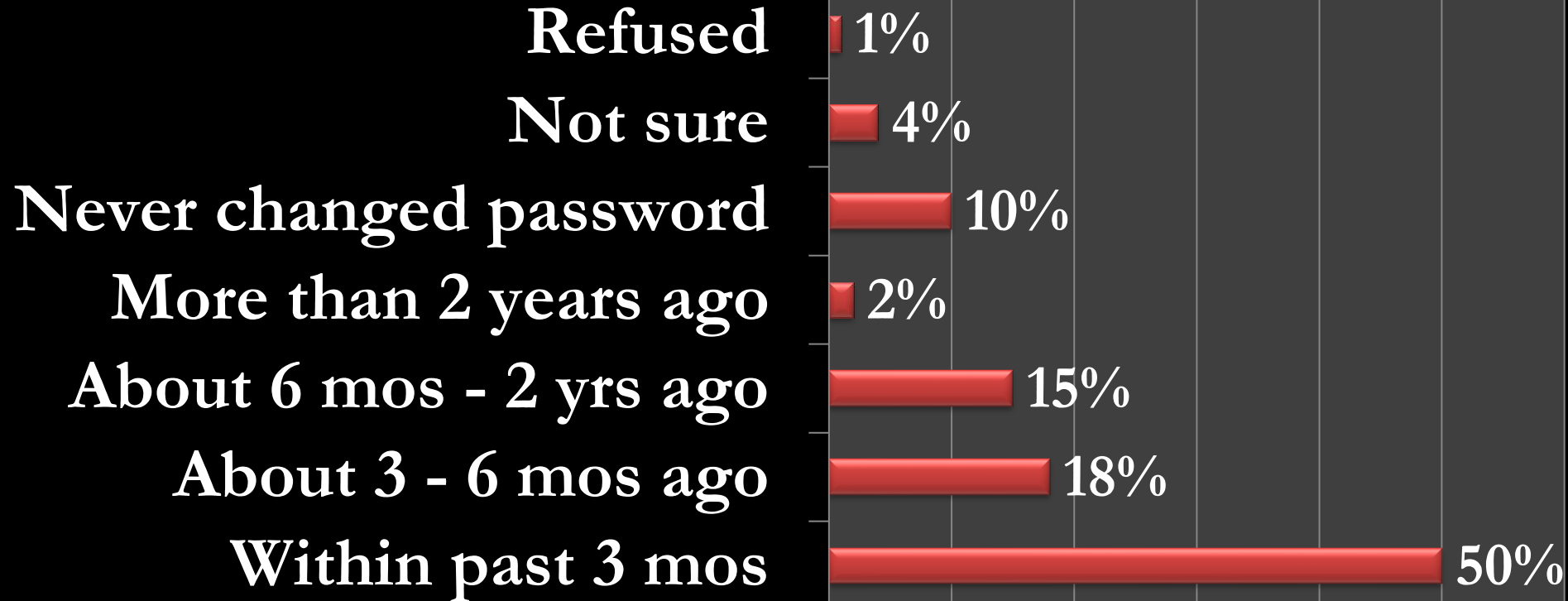
RISK FACTORS - not monitoring online banking



**FRAUD
WATCH**
NETWORK
AARP Real Possibilities

Identity Theft - online

RISK FACTORS - not changing passwords



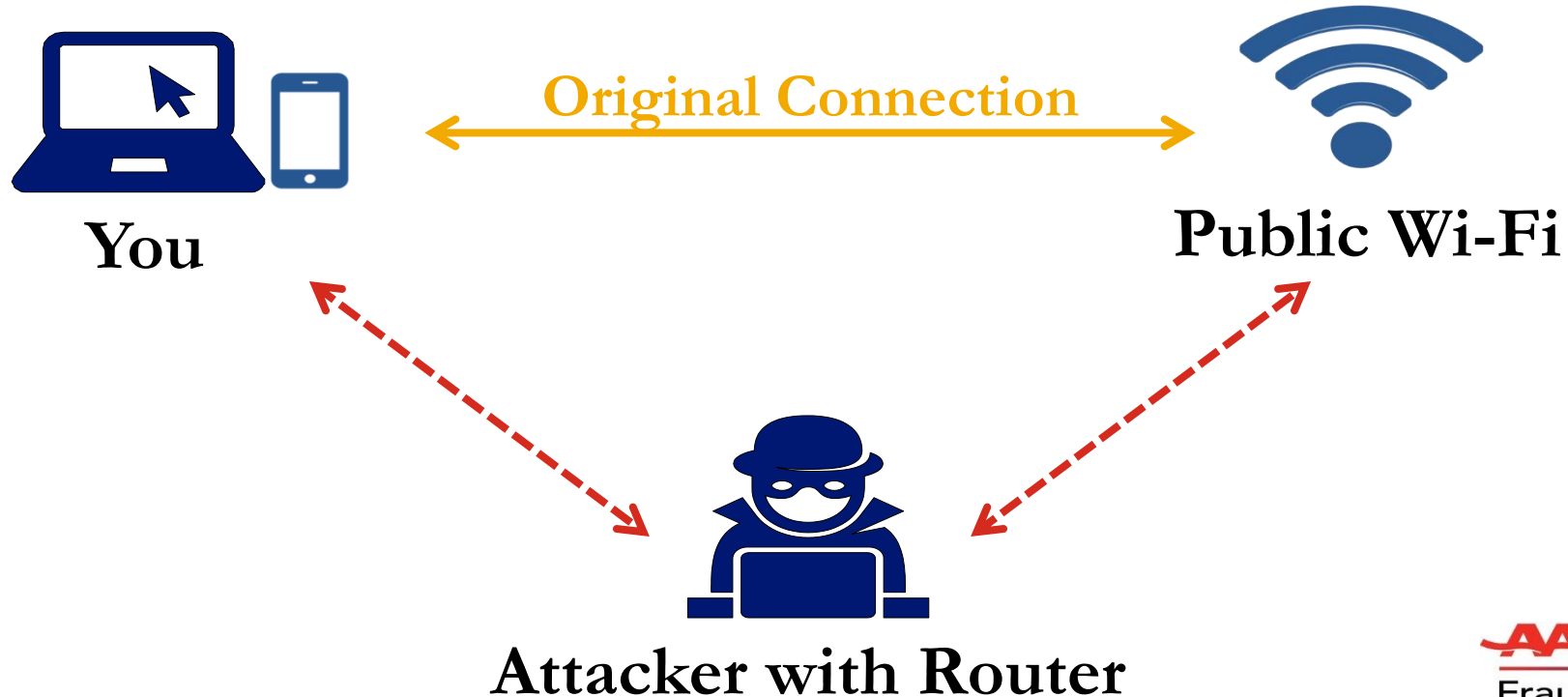
Identity Theft - online

RISK FACTORS – not protecting your computer



Identity Theft - online

RISK FACTORS – “Man in the Middle”



Identity Theft - online

RISK FACTORS – “Evil Twin”



Identity Theft - online

RISK FACTORS – “Wardriving”



Identity Theft - online

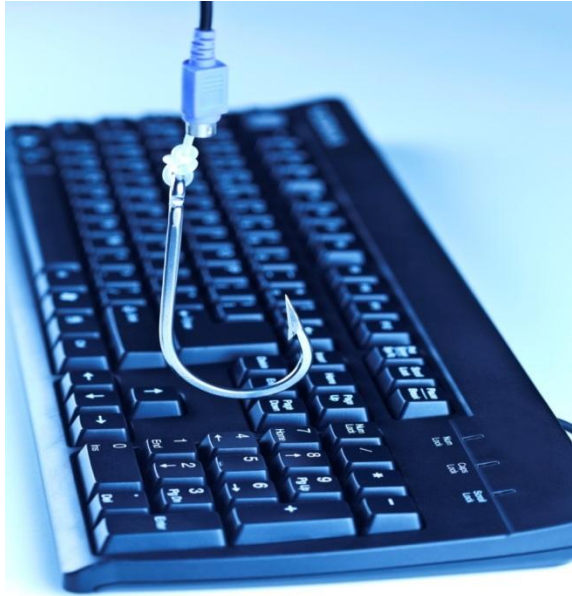
RISK FACTORS – “Phishing”

You are contacted via different means and asked to confirm sensitive information

- Text messages, phone (spoofing), online, email...
- New Medicare cards being issued
- IRS, closure of utilities, Social Security, tax filing
- Skimming (gas stations); debit card vs credit card
- Online banking vs hard copy banking

Identity Theft - online

TIPS: on avoiding phishing



- Don't click on the link!
- Don't open files from strangers
- If a message sounds too good to be true, it probably is
- Strange message from a friend?
Be wary
- Thoroughly read messages
- https = secure

Identity Theft - online

TIPS: on using public Wi-Fi



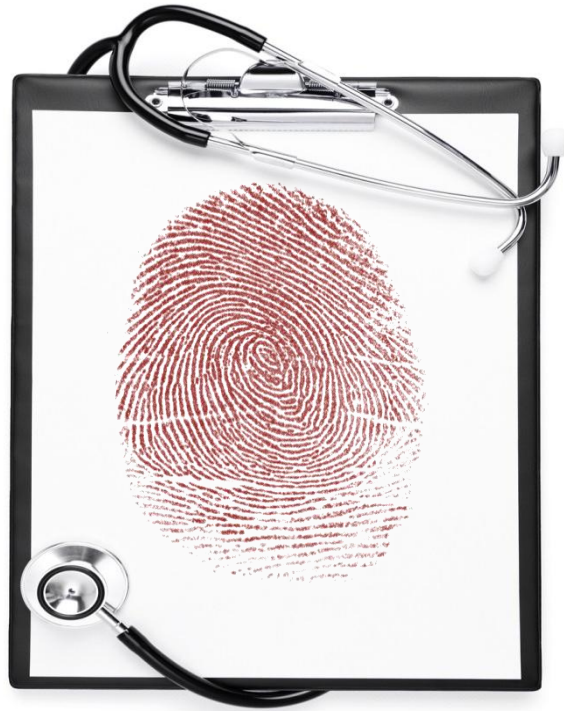
- Don't access sensitive information over public Wi-Fi
- Verify the true public Wi-Fi network name before logging on
- Secure your home Wi-Fi

Identity Theft - online

TIPS: other steps you can take



- 1 Monitor your accounts online
- 2 Secure your passwords
- 3 Protect your computer
- 4 Control your surfing
- 5 Watch for fake connections
- 6 Beware of phishing scams



Identity Theft - medical

Identity Theft - medical

WHAT IS IT?



Identity Theft - medical

WARNING SIGNS



A bill for services you didn't receive



Debt collector



Notice you reached your benefit limit



Denial of insurance

Identity Theft - medical

WAYS MEDICAL IDENTITY IS STOLEN



Data Breach



Phishing



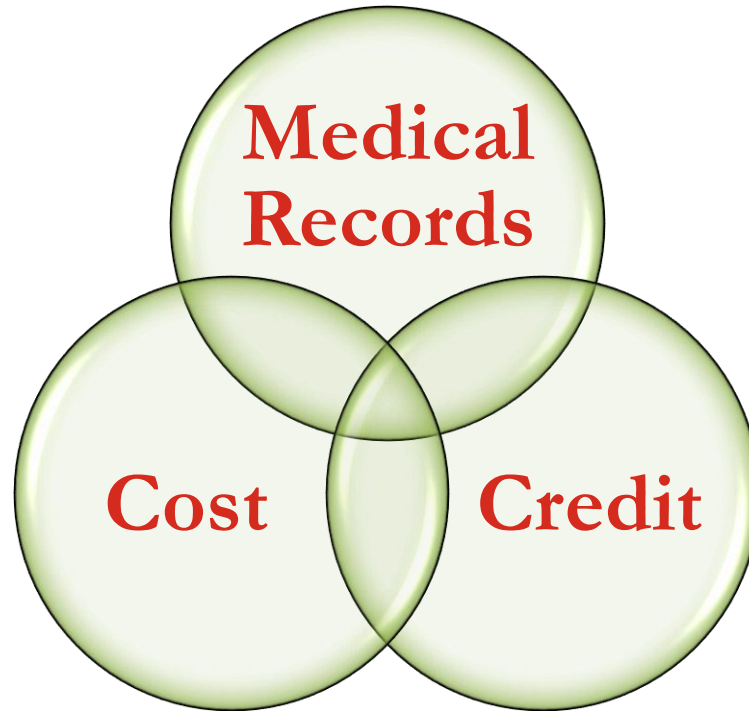
Dumpster Diving



"Free" Medical Services

Identity Theft - medical

IMPACT



Identity Theft - medical

TIPS (1)

- **Read medical and insurance statements**
 - ✓ Review Explanation of Benefits or Medicare Summary Notice.
 - ✓ Check provider name, date of service, and service provided.
 - ✓ Report discrepancies to insurance provider.
 - ✓ Protect your health plan or Medicare ID number.

Identity Theft - medical

TIPS (2)

- Be wary of offers for “free” health services or products requiring sharing health plan ID #.
- Don’t overshare health-related matters on social media.
- Sign up for online access with your insurance provider to avoid someone else doing it.
- Medicare doesn't call, visit, or email you.

Identity Theft



**3 ways to keep your
Social Security number
out of the wrong hands**

- Phone calls from 'SS'? Do not divulge any sensitive information
- Shred documents with SS number on them
- When asked for SS number, ask why they need it?

Identity Theft - medical

TIPS (3)

- Check your credit reports regularly
www.annualcreditreport.com



Identity Theft - medical

IF YOUR MEDICAL ID IS STOLEN

- Free credit monitoring
- Contact insurance provider
- File a police report
- Request your medical records
- If Medicare-related, report it to Office of Inspector General: 1-800-447-8477 / [OIG.HHS.gov/fraud/hotline](https://www.oig.hhs.gov/fraud/hotline)



Prevention Strategies

Prevention Strategies

TIPS (1)

- **What Cons agree on victims:**
 - ✓ Get Excited Easily and Act on Impulse
 - ✓ Don't Consider Why it's a Scam, Just Focus on Making Money
 - ✓ Don't Ask Questions, They Answer Questions
 - ✓ Don't Read Information, Rely on Sales Pitch



Prevention Strategies

TIPS (2)

- **Never make a buying decision in a heightened emotional state.**
- **Ask more questions than you answer.**
- **Read about the product before buying.**
- **Don't let the sales person control you.**
- **Develop a refusal script:**



Prevention Strategies

TIPS (3)

- **Protect Your SSN & Personal Information**
- **Monitor Your Bills & Financial Accounts**
 - ✓ www.finra.org/brokercheck
 - ✓ www.sec.gov
- **Watch Over Your Credit Reports**
 - ✓ www.annualcreditreport.com
 - ✓ 877-322-8228



Prevention Strategies

TIPS (4)

- **Protect PINs & Passwords**
- **Protect Your Information Online**
 - ✓ spam@uce.gov
 - ✓ “https” for More Secure Websites
- **Protect Your Mail**
 - ✓ www.optoutprescreen.com
 - ✓ 888-5-OPT-OUT
 - ✓ www.dmachoice.org



Prevention Strategies

TIPS (5)

➤ Be Cautious of Scams & Frauds

- ✓ Sign Up for Do-Not-Call Registry
(www.donotcall.gov, 888-382-1222)
- ✓ Double-Check References
- ✓ Verify Charities
(www.charitywatch.org;
www.charitynavigator.org)





Resources

OTHER (1)

- The National Association of Attorneys General (www.na.ag.org)
- FINRA Investor Education Foundation (www.saveandinvest.org)
- The North American Securities Administrators Association – NASAA (www.nasaa.org)



Resources

OTHER (2)

- U.S. Postal Inspection Services
(www.deliveringtrust.com)
- FTC Consumer Sentinel Hotline
(877-701-9595)
- Securities and Exchange Commission
(www.sec.gov/investor,
www.investor.gov, 800-SEC-0330)



Resources

OTHER (3)

- Consumer Financial Protection Bureau
(www.consumerfinance.gov/complaint)
- National Association of Insurance Commissioners
([www.naic.org/state\)web.map](http://www.naic.org/state)web.map))
- Medicare-related: Office of Inspector General: 1-800-447-8477 / OIG.HHS.gov/fraud/hotline



Resources

FRAUD WATCH NETWORK & CALL CENTER

➤ AARP Fraud Watch Network

- ✓ www.aarp.org/fraudwatchnetwork
- ✓ Access Information & Resources
- ✓ Receive Watchdog Alerts
- ✓ Read Stories
- ✓ Get Help

➤ Fraud Fighter Call Center

- ✓ 877-908-3360
- ✓ Counseling, support & referral services





Fraud Watch Network

Thank you!