



# IDENTITY THEFT, SCAMS AND FINANCIAL EXPLOITATION OF OLDER ADULTS

## A TRAINING FOR SERVICE PROVIDERS AND PROFESSIONALS

PRESENTED BY THE ONONDAGA COUNTY ELDER IDENTITY THEFT COALITION

*THIS POWER POINT WAS PRODUCED BY THE OCEITC UNDER AWARD #2016-XV-GX-K004, AWARDED BY THE OFFICE FOR VICTIMS OF CRIME, OFFICE OF JUSTICE PROGRAMS, U.S. DEPARTMENT OF JUSTICE. THE OPINIONS, FINDINGS, AND CONCLUSIONS OR RECOMMENDATIONS EXPRESSED IN THIS POWER POINT ARE THOSE OF THE CONTRIBUTORS AND DO NOT NECESSARILY REPRESENT THE OFFICIAL POSITION OR POLICIES OF THE U.S. DEPARTMENT OF JUSTICE.*

# GOALS

- Define Elder Abuse, Financial Exploitation, and Identity Theft
- Common Scams
- Organizational Practices
- Victim assistance
- Prevention
- Resources

# ELDER ABUSE

- Physical Abuse
- Emotional Abuse
- Sexual Abuse
- Neglect
- Financial Exploitation

Be aware that these types of abuse may co-occur

# FINANCIAL EXPLOITATION

- New York State Social Services Law, Section 473, subsection 6(g) defines Financial Exploitation as:  
the improper use of an adult's funds, property or resources by another individual,  
including but not limited to, fraud, false pretenses, embezzlement, conspiracy, forgery,  
falsifying records, coerced property transfers or denial of access to assets.

# IDENTITY THEFT

- Identity theft is a crime that involves the illegal access and use of an individual's personal and/or financial information.
  - May affect: credit, banking, taxes, financial obligations, health care, etc.
- This information can be obtained in many ways including: unauthorized use, theft, dumpster diving, credit card skimming, phishing, hacking and scams.

# PERPETRATORS

- Family/Relatives
- Friends and/or Neighbors
- Caretakers
- Professionals – ie Attorneys, Financial Advisors
- Any person in a position of trust
- Strangers/scammers

## THE COST

- In 2016, annual financial costs of Financial Exploitation in New York State is estimated to be up to \$1.5 billion. (Source: New York State Cost of Financial Exploitation Study)



## ACCORDING TO THE FEDERAL TRADE COMMISSION (FTC) IN 2019:

- Imposter Scams was the #1 consumer complaint to the FTC in the US
- Identity Theft was the #1 consumer complaint to the FTC in NYS
- NYS ranked 9<sup>th</sup> in imposter scam complaints
- Adults 60 and older filed 37% of all fraud complaints nationwide
- Fraud loss for adults 60 and older was \$444 million
- The median financial loss for adults 60 and older was \$1,000 per person



# ITAP REPORT 2018

- The Identity Threat Assessment and Prediction (ITAP) model key takeaways include:
  - 75% of victims experienced emotional distress
  - 50% of incidents involving high emotional distress are perpetrated by insiders (ie family members)

# THERE ARE MANY SCAMS OUT THERE INCLUDING....

- Fake Check, Foreign Lottery or Sweepstakes Scams
- Home Repair Scams
- Grandparent Scams
- Sweetheart Scams
- Social Security Scams
- IRS Scams

This is not an exhaustive list!

## HOW DOES IT WORK?

- Scam artists use a “hook” to trick individuals into providing information and/or sending money
- Scammers prey on an older adult’s feelings of love, goodwill and/or fear
- Older adults may be hesitant to reach out for help

# FAKE CHECK, FOREIGN LOTTERY, OR SWEEPSTAKES SCAMS

CONGRATULATIONS!! YOU WON!!



# HOME REPAIR SCAMS

Offers to make improvements/repairs. May be door-to-door sales.  
A deposit or full price is paid. Work never starts or completed.



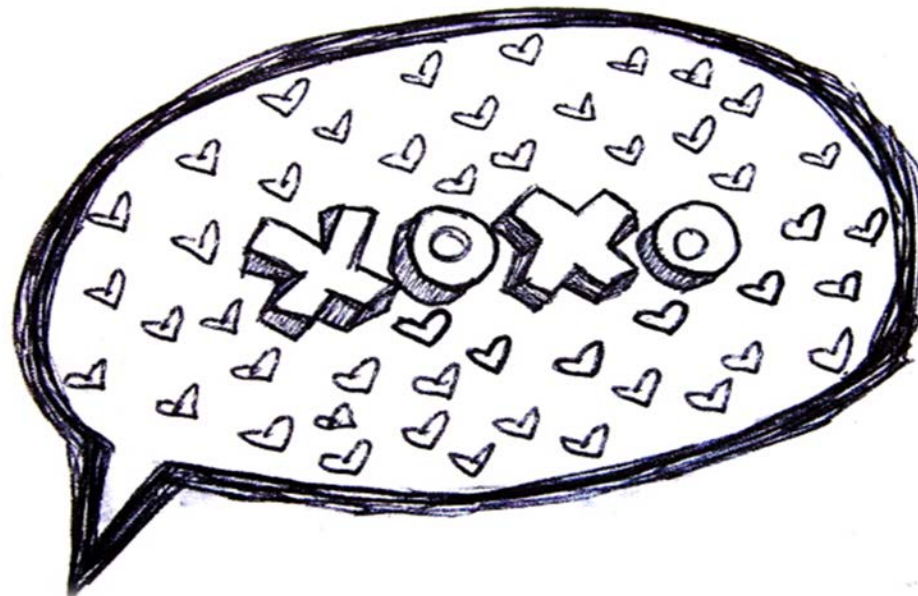
# GRANDPARENT SCAMS



“Grandma I’ve been arrested! Wire money so I can get out of jail. Please don’t tell mom and dad.”

# SWEETHEART SCAMS

Scammer befriends the victim.



# SOCIAL SECURITY SCAMS

“Contact us right away or your social security benefits will be suspended.”





# IRS SCAMS

“You have overdue taxes. You will be arrested if you do not make payment today.”



# OLDER ADULTS ARE TARGETED BECAUSE...

- May be more vulnerable – isolation and loneliness
- May have more assets (money, home, car, jewelry, etc.)
- May have cognitive limitations
- May be more trusting
- Prey on feelings of love, goodwill and/or fear
- May have difficulty adapting to changes in technology or schemes
- May not report fearing loss of independence

# IMPACT ON OLDER VICTIMS

- Loss of trust in others
- Loss of security and independence
- Feelings of fear, shame, guilt, anger
- Depression and isolation
- Financial hardship
- Becoming reliant on others and/or government programs

# VICTIM INDICATORS

- Their money/assets are disappearing
- They tell you someone is asking them for money
- Mail is unopened and/or piling up
- Bills are not being paid or they have unexplained bills
- They are denied credit for no apparent reason
- They have a new friend who is now requesting help, taking money or other assets, or otherwise influencing the victim
- They have recently changed important legal documents (ie Power of Attorney or Will)
- There are unexplained transactions on bank or other financial accounts
- ATM transactions when the victim does not leave their home
- They are being contacted by bill collectors
- Behavioral cues indicating distress

# ORGANIZATIONAL PRACTICES

- The University of Texas at Austin - Center for Identity was established “to serve as a center of excellence in identity management, privacy, and security delivering actionable knowledge and resources”
- “Identity” is whom someone or what something is, for example, the name by which something is known
- Personal Identifying Information (PII) is an asset

Source: The University of Texas at Austin – Center for Identity

# ATTRIBUTES OF PII

- Attribute: small pieces of information that make up a digital identity
- Key word is “Identifiable”
- There are many ways to identify people, devices, and organizations
- For example:
  - Information about an individual (name, date of birth, social security number)
  - Data that identifies a specific individual

Source: The University of Texas at Austin – Center for Identity

# WHAT IS YOUR IDENTITY ASSET INVENTORY?

- What type of Identity assets does your organization hold?
- Where are those Identity assets located?
- Who has access to those Identity assets?
- Are those Identity assets monitored?

Source: The University of Texas at Austin – Center for Identity

# PROTECTING PII

- 99.7% of incidents where personally identifiable information was compromised is local (ITAP - 2018)
- What information are you collecting and why?
- How is that information stored, used and/or shared?
- What are you doing to protect identity assets?
  - Privacy policy
  - Clients
  - Employees
  - Donors

Source: The University of Texas at Austin – Center for Identity



# STRATEGIES FOR MANAGING RISK

## Recommendations:

1. Take an inventory of your identity assets
2. Evaluate the value of your identity assets
3. Determine your identity asset vulnerabilities
4. Develop a policy to protect your identity assets
5. Create a plan to respond if an incident occurs

Source: The University of Texas at Austin – Center for Identity

# HOW YOU CAN HELP

- Educate yourself and those you serve on common schemes and methods of prevention
- Watch for signs that fraud may have occurred
- Help victims report identity theft and scams
- Understand how a victim's emotional, mental and physical health may be affected
- Be aware of resources and make referrals

Respond non-judgmentally, with compassion and respect

# VICTIM RESPONSE/ACTION STEPS

May include...

1. Place a Fraud Alert on credit reports
2. File a Police Report
3. Close accounts (bank, credit) that are known or believed to have been compromised
4. File a complaint with the Federal Trade Commission (FTC)
5. Review copies of credit reports and account statements regularly, and correct any errors promptly
6. Report to other agencies as needed (ie IRS, social security, health insurance provider)
7. Refer to Taking Action: An Advocate's Guide to Assisting Victims of Financial Fraud

# CREDIT REPORTING AGENCIES

- Equifax 1-800-525-6285 or [www.equifax.com](http://www.equifax.com)
- Experian 1-888-397-3742 or [www.experian.com](http://www.experian.com)
- TransUnion 1-800-680-7289 or [www.transunion.com](http://www.transunion.com)
- Annual Credit Report 1-877-322-8228 or [www.annualcreditreport.com](http://www.annualcreditreport.com)
- You are entitled to a credit report once a year at no charge from all 3 credit reporting agencies
- If you file a fraud alert with one credit reporting agency they must notify the other two; lasts for one year
- Credit freeze

# PREVENTION TIPS

- Use PINS or Passwords on all accounts (bank, credit cards, cell phone, internet)
- Do not give out personal information- on the phone, in the mail, or on the internet- unless you know who you are dealing with
- Shred personal information, credit card offers, etc.
- Consider other options instead of commercial credit cards
- Consider how mail is sent
- Do not give out social security number unless absolutely necessary
  - Ask:
    - Why do you need it?
    - How will you use it?
    - How will you protect it from being stolen?
    - What will happen if I do not give it to you?
- Consider inviting a trusted “second set of eyes”

## LIMIT CONTACT

- Do Not Call Registry: 1-888-382-1222 or [www.donotcall.gov](http://www.donotcall.gov)
- Opt out of credit card offers: 1-888-567-8688 or [www.optoutprescreen.com](http://www.optoutprescreen.com)
- Robo-call blocking: [Nomorobo.com](http://Nomorobo.com)

# A VICTIM CENTERED RESPONSE

- Respond with compassion and respect
- Validate help-seeking as a proactive form of self-care
- Help a victim set realistic expectations
- Assess safety concerns

# RESOURCES

- Local Resources:
  - Adult Protective Services (APS) – (315) 435-2815 or [www.ongov.net/adult/protective](http://www.ongov.net/adult/protective)
  - Syracuse Jewish Family Service - (315) 446-9111 or [www.sjfs.org](http://www.sjfs.org)
  - Syracuse Regional Attorney General's Office – (315) 448-4848 or [www.ag.ny.gov/syracuse-regional-office](http://www.ag.ny.gov/syracuse-regional-office)
  - Vera House - (315) 468-3260 or [www.verahouse.org](http://www.verahouse.org)
- National Resources:
  - Cybercrime Support Network – [www.fraudsupport.org](http://www.fraudsupport.org)
  - Identity Theft Resource Center (ITRC) – 1-888-400-5530 or [www.idtheftcenter.org](http://www.idtheftcenter.org)
  - Federal Trade Commission (FTC) – 1-877-438-4338 or [www.ftc.gov](http://www.ftc.gov)





# QUESTIONS?

