
IDENTITY THEFT, SCAMS AND FINANCIAL EXPLOITATION OF OLDER ADULTS

A TRAINING FOR LAW ENFORCEMENT MODULE I – OVERVIEW

PRESENTED BY THE ONONDAGA COUNTY ELDER IDENTITY THEFT COALITION

THIS POWERPOINT 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.

OBJECTIVES

- Objectives of this module include:
 - Defining Elder Abuse, Financial Exploitation, and Identity Theft
 - Who are the Perpetrators?
 - List of Common Scams
 - Victim Indicators
 - Local and National Resources

ELDER ABUSE

- There are five categories we include when defining elder abuse. They are:
 - Physical Abuse – these are “hands on” offenses such as hitting, punching, kicking, and shoving.
 - Emotional Abuse (may also be referred to as Verbal Abuse or Psychological Abuse) – these are the words, insults and threats, for example “you are stupid”: “if you didn’t have me, you wouldn’t have anyone”; or “if you don’t do what I say, I am going to put you into a nursing home”. Isolation can be another form of emotional abuse.
 - Sexual Abuse – may be “hands on” or “hands off” offenses including rape, rough handling of the genital area, and forcing an older adult to watch pornography.
 - Neglect – this is an inaction – an individual takes on the responsibility of caring for another and fails to do so.
 - Financial Exploitation – definition on next slide.

Be aware that these types of abuse most often co-occur, so when you see one, there could be more.

FINANCIAL EXPLOITATION

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

IDENTITY THEFT

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

WHO ARE THE PERPETRATORS?

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

Most financial crimes are committed by family members or others known by the victim.

We tend to hear more about scams by strangers because they are more often reported and may be “newsworthy”.

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

Please be aware that this is not an exhaustive list!

- We will explore these scams in greater detail in Module 2.

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.

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.
- Respond non-judgmentally, with compassion and respect.
- Be aware of resources and make referrals.

RESOURCES

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

QUESTIONS

1. Elder Abuse includes physical abuse, emotional abuse, sexual abuse, neglect, and financial exploitation. True or False?
2. Most financial crimes are committed by family members or others known by the victim. True or False?

IDENTITY THEFT, SCAMS AND FINANCIAL EXPLOITATION OF OLDER ADULTS

A TRAINING FOR LAW ENFORCEMENT

MODULE 2 – COMMON SCAMS

PRESENTED BY THE ONONDAGA COUNTY ELDER IDENTITY THEFT COALITION

THIS POWERPOINT 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.

OBJECTIVES

- Provide a basic understanding of Common Scams
- Describe how these scams work
- Understand why older adults are targeted

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! Scammers are clever and new scams are reported every day!

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.

OLDER ADULTS ARE TARGETED BECAUSE...

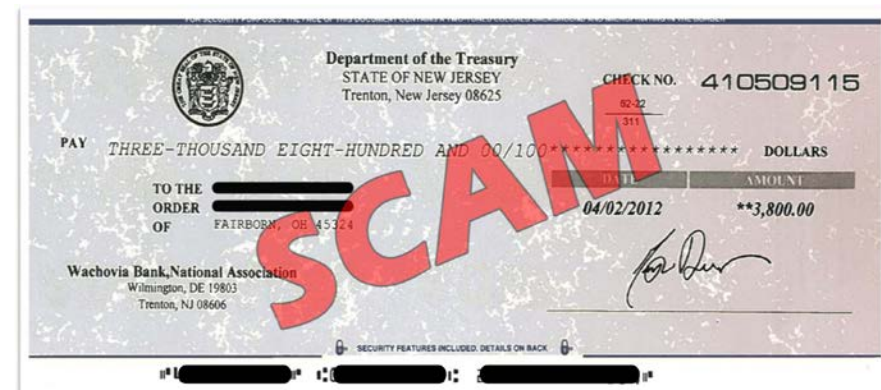
- They may be more vulnerable due to isolation and loneliness.
- They may have more assets (money, home, car, jewelry, etc.)
- They may have cognitive limitations.
- They may be more trusting.
- They may have difficulty adapting to changes in technology or schemes.
- They may not report fearing loss of independence.

Remember: Scammers prey on an older adult's feelings of love, goodwill and/or fear.

FAKE CHECK, FOREIGN LOTTERY, OR SWEEPSTAKES SCAMS

This scam can take many forms. For example....

1. An older adult may get a fake check in the mail. If they cash it, the check will bounce and the scammer then gets the victim's bank information. If in doubt, research the check's authenticity (i.e. take the check to a bank for verification).
2. In a foreign lottery scam the older adults is notified via phone or mail they have won a lottery or sweepstakes, but they must first send a payment for taxes, and thereafter the winnings will be sent to them. In legitimate lotteries and sweepstakes, taxes are deducted before the winnings are awarded. Also inquire if the older adult entered, because you cannot win what you do not enter.



HOME REPAIR SCAMS

This scam involves an unsolicited offer to make home improvements and/or repairs. Typically it is presented as a door-to-door sales offer. A deposit or full price is paid for work, but then the work is either never started or not completed.



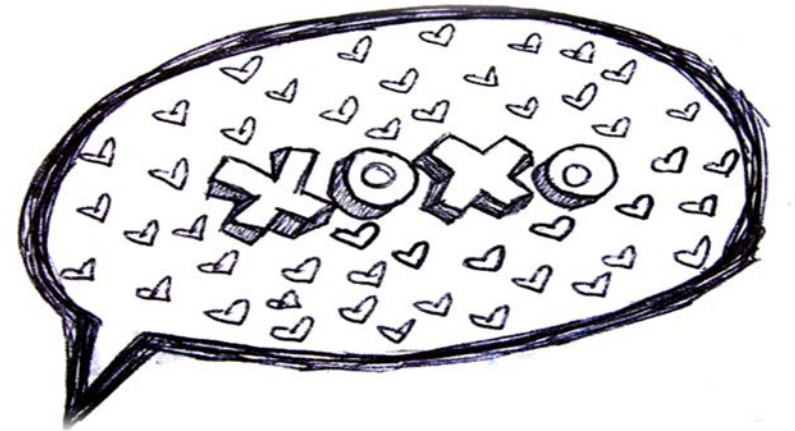
GRANDPARENT SCAMS

In this scam the older adult gets a phone call, and the person on the other end of the line says something like “Grandma I’ve been arrested! I need you to wire me money so I can get out of jail. Please don’t tell Mom and Dad.” This call often happens in the middle of the night, waking the older adult. The older adult may be startled and confused. Also secrecy can be a red flag.



SWEETHEART SCAMS

Sweetheart scams occur when the scammer befriends the victim. This can happen in person or online. The victim may believe the scammer is their boyfriend/girlfriend. These scams may be effective because the victim is lonely or isolated.



SOCIAL SECURITY SCAMS

In this scam the victim receives a phone call and the person on the phone tells them there is an issue with their social security benefits and requests their social security number to clear it up or, if there is no answer, will leave a message to contact them right away or their social security benefits will be suspended. Be aware that the Social Security Administration will not call an individual if there is an issue; the initial contact will always be in writing.



IRS SCAMS

The IRS scam is similar to the Social Security scam in that the victim gets a phone call whereby the caller claims to be from the IRS and tells the victim something like “You have overdue taxes. You will be arrested if you do not make payment today.” The IRS will not call an individual if there is an issue; the initial contact will always be in writing.



QUESTIONS?

1. Scammers prey on an older adult's feelings of love, goodwill and/or fear. True or False?
2. Older adults are targeted because they may be more vulnerable due to isolation and loneliness. True or False?

IDENTITY THEFT, SCAMS AND FINANCIAL EXPLOITATION OF OLDER ADULTS

A TRAINING FOR LAW ENFORCEMENT

MODULE 3 – IMPACT AND PREVENTION

PRESENTED BY THE ONONDAGA COUNTY ELDER IDENTITY THEFT COALITION

THIS POWERPOINT 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.

OBJECTIVES

- Objectives of this module include:
 - Understand the cost and statistics related to Identity Theft, Scams and Financial Exploitation of Older Adults
 - Learn the Impact of Identity Theft, Scams and Financial Exploitation on Older Adults
 - Learn Victim Response/Action Steps
 - Learn Prevention Practices

THE COST

- In 2016, annual financial costs of financial exploitation of older adults 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 2018:

- 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 13th in identity theft complaints.
- Adults 60 and older filed 65,134 identity theft complaints (15%) nationwide.
- Fraud loss for adults 60 and older was \$393 million.
- The average financial loss for adults 60 and older was \$3,058 per person.

THE IMPACT ON OLDER VICTIMS

Older adults who have been the victim of identity theft, scams or financial exploitation may experience:

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

IF AN INDIVIDUAL HAS BEEN A VICTIM

Response/Actions steps a Victim can take include:

1. Place a Fraud Alert on credit reports with credit reporting agencies.
2. File a Police Report, which will help to document the victim's claim.
3. Close accounts (bank, investment, 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 (i.e. IRS, social security, health insurance provider).
7. Encourage victims to contact local resources (APS, Syracuse Jewish Family Service and/or Vera House) for assistance with any of these steps.

CREDIT REPORTING AGENCIES

There are 3 credit reporting agencies:

- Equifax 1-800-525-6285 or www.equifax.com
- Experian 1-888-397-3742 or www.experian.com
- TransUnion 1-800-680-7289 or www.transunion.com

To place a **fraud alert**, an individual can contact one of the 3 credit reporting agencies listed above. If a fraud alert is filed with one credit reporting agency, that agency must notify the other two. A fraud alert lasts for one year.

An individual is entitled to a free credit report once a year from all 3 credit reporting agencies.

An individual may also request a **credit freeze**. This stops all attempts to access and get credit in that individual's name by anyone - including that individual- until they lift the freeze.

PREVENTION TIPS

The following precautions can help reduce the risk of identity theft, scams and financial exploitation of older adults:

- Use PINS or complex passwords on all accounts (i.e. 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.
- Do not send mail from personal mailbox. Drop it off at the post office or deposit in a blue post office receptacle.
- Do not give out social security number unless absolutely necessary.
- Consider inviting a trusted “second set of eyes” to review bills, credit reports, and other important documents.

LIMIT CONTACT

An individual can also limit contact from unsolicited offers and calls by:

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

A VICTIM CENTERED RESPONSE

When responding to an older adult who has been the victim of identity theft, scams and financial exploitation, remember:

- Respond with compassion and respect.
- Assess safety concerns.
- Take a police report.
- Help a victim set realistic expectations.
- Refer victims to APS, Syracuse Jewish Family Service and/or Vera House.
- Validate help-seeking as a proactive form of self-care.

QUESTIONS?

1. In 2016, annual financial costs of Financial Exploitation in New York State is estimated to be up to \$1.5 billion. True or False?
2. A precaution that can help reduce the risk of identity theft, scams and financial exploitation of older adults is to use a password on accounts. True or False?

IDENTITY THEFT, SCAMS AND FINANCIAL EXPLOITATION OF OLDER ADULTS

A TRAINING FOR LAW ENFORCEMENT

MODULE 4 – INVESTIGATION AND RESPONSE

PRESENTED BY THE ONONDAGA COUNTY ELDER IDENTITY THEFT COALITION

THIS POWERPOINT 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.

OBJECTIVES

- Objectives of this module include:
 - Understanding Methods of Financial Exploitation
 - Crimes Related to Financial Exploitation
 - Interviewing – Who and What
 - Evidence Collection
 - Investigation Strategies

METHODS OF FINANCIAL EXPLOITATION

- Scams
- Identity theft / Synthetic Identity Theft (use of multiple different pieces of identity to create one fictitious ID)
- Theft
- Coercion and extortion
- Fraud and deception
- Abuse of legal authority (i.e. Power of Attorney)
- Manipulation

CRIMES RELATED TO FINANCIAL EXPLOITATION

- Larceny (PL 155.25, 155.30, 155.35, 155.40, 155.42)
- Fraudulently obtaining a signature (PL 165.20)
- Forgery (PL 170.05, 170.10, 170.15)
- Scheme to defraud (PL 190.60, 190.65)
- Identity Theft (PL 190.78, 190.29, 190.80)
- Tampering with a witness (PL 215.10, 215.11, 215.12, 215.13)
- Intimidating a victim or witness (PL 215.15, 215.16, 215.17)
- Endangering Welfare (PL 260 section Elderly 260.(31)(32)(34))
- Effective December 18, 2013, financial crimes were added to the list of family offenses (Chapter 526):
- Chapter 526
 - Adds **identity theft, larceny and coercion** to the list of family offenses, allowing victims to seek relief and an order of protection in Family Court, as well as Criminal Court.
 - Subject to mandatory arrest and the order of protection will be added to the statewide order of protection registry.
 - Adds a new condition that can be included in orders of protection that requires the abuser to return specified “identification documents,” such as a passport, immigration documents, birth certificate, benefits/ insurance cards, bank or credit cards etc., to the protected party.

WHO TO INTERVIEW

- Victim
- Suspect
- Family members
- Neighbors
- Victim's health care providers
- Psychiatrist
- Victim's pharmacist
- Victim's lawyer
- Bank employees
- Adult Protective Services (APS)
- Accountant / Financial Advisor

WHAT TO ASK/OBTAIN DURING INTERVIEWS

- Identify all existing financial accounts (assess capacity during victim interview).
- Has the victim signed any documents and what were they? Did the victim understand what they were signing?
- Is the victim performing any financial tasks for anyone (purchasing gift cards, opening new bank accounts, sending receiving financial documents, performing financial transactions)?
- Is there a Power of Attorney (POA) involved and if so what are the details? Was there a former or prior POA and if so, why the change?
- Has the victim made any new friends or acquaintances (if so, what are the circumstances)?
- Identify all financial obligations, bills, expenses, etc.
- Identify all persons who assist victim and their role (i.e. housework, aides, finances, POA).
- Who accompanies the victim to appointments? Has anything changed recently?
- Have the victim's medications changed or have there been other changes (i.e. victim not refilling a medication at regular time – indicative of victim stopping a medication or medication taken away from victim)?
- Consider obtaining formal evaluation from medical provider including financial decision making ability.
- Observations regarding victim's cognitive ability or any recent change(s) – may include medical professional or medical notes, bank teller, financial advisor, etc.
- When possible obtain specific dates and times for any details obtained during interviews to assist in establishing timelines.

EVIDENCE COLLECTION

- Checkbooks and registers
 - Overdue or unpaid bills
 - Bank statements of victim and suspect
 - Tax records
 - Receipts for purchases
 - ATM transactions
 - Surveillance footage at bank,ATMs
 - Credit card statements
 - Credit reports
 - Data off home or work computers
 - Power of Attorney and other legal documents
 - Medical records of victim
 - Capacity evaluation of victim
 - Mental health and substance abuse treatment records of suspect
 - Employment records for suspect
 - Toxicology screen for victim
 - Prescription records of suspect and victim
- **Identify what evidence requires a subpoena and/or search warrant and submit.**

FINANCIAL INDUSTRY / BANK SECRECY ACT / CRIMINAL INVESTIGATIONS

- **Bank Secrecy Act (BSA)** – sets forth a system of reporting and recordkeeping requirements in financial institutions designed to help track large and/or suspicious financial transactions.
- BSA requires certain reports to be filed by financial institutions, two of which can be helpful to a criminal investigation: Currency Transaction Report (CTR) and Suspicious Activity Report (SAR).
- **Currency Transaction Report (CTR)** – reports cash transaction exceeding \$10,000.
- **Suspicious Activity Report (SAR)** – reports suspicious activity on a financial account exceeding \$5,000 to include but not limited to fraud, financial crimes, and structuring. SAR data is available to law enforcement and can be an effective source of data for financial investigations.
- **Financial Crimes Enforcement Network (FinCen)** – responsible for overseeing and enforcing BSA reporting requirements and the collection, analysis, and reporting of financial crimes analysis (CTR/SAR).

FINANCIAL INSTITUTIONS / RECORDS / DOCUMENTS

Account Signature Cards – Who is authorized to sign on the account.

Account Statements – Summarized history of transactions that can assist in identifying activity patterns, debit and credits. Typically a starting point for tracing funds into and out of victim or suspect accounts.

Canceled Checks – Assists in tracing financial activity, identify parties involved in disbursements – pay attention to signatures, memo line and deposit bank on back of check (follow \$).

Wire Transfers – incoming and/or outgoing, identify beneficiary bank and party. Victims of scams often convinced to use this method of transferring funds. Pay attention to accounts and follow \$.

ACH (Automated Clearing House) payment – method of electronic payment to and from a bank account. Typically only requires a name, bank routing number and bank account number. Popular method of transferring funds with identity theft fraud schemes.

Power of Attorney (POA) / Joint Account – Identify any POA or Joint Account activity. This is important financial information when investigating elder financial exploitation, identity theft, account takeover, etc. Recommend consult prosecuting attorney when POA and/or joint account involved.

- Date(s) involved – compare to victim decision making capacity.
- What does it cover?
- Any other current or prior POAs – do they know and/or why are they no longer POA?

INVESTIGATION / ANALYZING THE DATA

- **The type of fraud** and the **jurisdiction of occurrence often dictates your investigative response**. Many investigations involving older victims are complex and require not only probable cause but a thorough understanding of established evidence and how that evidence supports the overall investigation.
- **Timelines** between the specific fraud involved, financial records, medical records, and victim capacity assessments are often beneficial in supporting an investigation.
- **Identify the “Ins” and “Outs” (aka Deposits and Withdrawals)** with financial records – enlist assistance of forensic accountant and District Attorney’s office if necessary. Establish a summary of financial activity weekly/monthly depending on type of investigation.
- Consider a consultation with the **Onondaga County E-MDT** (Enhanced Multi-Disciplinary Team).
- **Compare and analyze the financial timelines** (suspect and victim) to timelines of victim medical records and timeline of fraud events to bolster evidentiary support.
- Example: Older adult victim of fraud by a caregiver – timelines establish that suspect manipulated POA documents, medications were not properly administered, victim diminished capacity occurred before suspect began their scheme, suspect began accompanying victim into financial institutions, suspect opened accounts in victims’ name and suspect’s financial lifestyle improved with no legitimate reason coinciding with victim events.

ISSUES THAT MAY ARISE DURING INVESTIGATION

- Agencies/Organizations for older adults often work in “silos” (Adult Protective Services, law enforcement, financial institutions, etc.).
- Partnering between agencies breaks down the silo and leads to a more effective investigation and victim response.
- Be aware of numerous financial accounts that may exist (financial institutions, financial advisors, etc.) - identifying often involves a tedious review of documents and effective initial review of victim’s bank statements. Access to a forensic account can be obtained through the E-MDT.
- Victim’s financial habits may not be readily visible in the initial bank documents – interviews with friends, family and review of other documentation can aid in determining habits.
- Victim may be involved in multiple scams with multiple perpetrators for a longer period of time than the initial information suggests.
- Difficulty locating financial accounts – look at the victim’s bank statement, check service providers for direct deposit accounts on file (cable, utility, social security, etc.).
- Type of fraud involved changes complexity of investigation (i.e. Synthetic Identity Theft involves a combination of fictitious and real stolen identities in order to create a new identity and new credit may be established under the new synthetic identity).

FEDERAL TRADE COMMISSION (FTC) / CONSUMER SENTINEL

- Important that victims of fraud, identity theft or unfair business practices file a consumer complaint with FTC in addition to reporting to the police. Particularly with any situation involving a scam.
- Data from these complaints is compiled into Consumer Sentinel database.
- Consumer Sentinel is a valuable investigative tool for law enforcement. It compiles data from millions of complaints for law enforcement to use in assessing fraud investigations.
- Data analysis can help you assess broader fraud schemes related to a local investigation, obtain suspect information, locate law enforcement agencies conducting similar investigations or targeting the same suspect in a larger fraud scheme, identify whether a point of compromise for a larger fraud scheme is in your jurisdiction.
- Free for law enforcement.
- Many common scams where victims seemingly send funds out of country now involve more suspects utilizing elaborate measures to mask their base of operations within the U.S. The Consumer Sentinel provides the data to allow you to properly assess if you have a large scale fraud scheme being organized and operated out of your jurisdiction.
- Contact at register.consumersentinel.gov or call the Consumer Sentinel Help Line at 1.877.701.9595.

HYPOTHETICAL INVESTIGATIVE BENEFITS FROM USE OF CONSUMER SENTINEL

- Older adult victim has been sending wire transfers as part of a scam after answering cold call for lower credit rate. The monetary loss is not large enough to warrant a full scale investigation at this time. The victim has been receiving phone calls from suspect from same spoofed phone number directing where to send the funds. You run the suspected phone number in Consumer Sentinel and find that there are dozens of victims nationwide involving that number totaling hundreds of thousands of dollars in loss. This allows you the option of referring your case to an agency conducting a more in depth investigation.
- Older adult victim's family reports their loved one has been the victim of a scam. They explain that there was only an initial loss but now their loved one is being paid. You assess financial records to identify incoming Western Union funds being received by the victim at a local store which are then deposited to the victims' bank account with multiple purchases of prepaid gift cards. However, you cannot find any indication that the gift cards or funds have been sent out from the victim. You query the victim data and Western Union address in the Consumer Sentinel and find that there are dozens of other older adult victims across the U.S sending funds via Western Union to this same location. This type of data strongly suggests the victim is now likely an unintentional money mule with suspects possibly operating out of your jurisdiction.

QUESTIONS?

1. Scams, coercion, and abuse of legal authority are all methods of financial exploitation. True or False?
2. Timelines between the specific fraud involved, financial records, medical records, and victim capacity assessments are often beneficial in supporting an investigation. True or False?