You have the power to Outsmart the scammers

Your name: ________________________________
Welcome
Program synopsis

Incidents of fraud are on the rise, and scammers’ tactics are becoming more complex. This presentation will help give you the information you need to Outsmart the Scammers.

During the program, we’ll discuss how to spot certain red flags that may indicate a fraudulent encounter, resources you can turn to in the event you or loved ones are targeted and steps you can take to help protect yourself and loved ones.

Seminar Contents

Fraud by the numbers ............................................. 3
Scenario 1: Collection fraud ................................. 4
Scenario 2: Grandparent scam ............................... 5
Scenario 3: Sweetheart scam ................................. 6
Scenario 4: Lottery/Sweepstakes scam ...................... 7
Scenario 5: Social Security scam ............................ 8
Other Red flags .................................................. 9
Protect yourself and those you love ........................... 10-11
Other resources available ................................. 12-13
Friend or fraud?
Scenario #1 .......................................................... 14
Scenario #2 .......................................................... 15
Scenario #3 .......................................................... 16
### Fraud by the numbers

| 9 million | More than 9 million Americans have their identities stolen each year, either individually or through a data breach, according to the Federal Trade Commission (FTC). |
| $36.5 billion | Fraud and financial abuse schemes targeting the elderly are growing problems in the United States that cost victims at least $36.5 billion annually, according to the National Council on Aging |
| 1 in 6 | Approximately one out of six elders age 60+ is victimized financially, according to the Department of Health & Human Services' National Council on Aging. |
| 1 in 24 | Only one out of 24 cases is reported, according to the National Center on Elder Abuse. |
| 90% | Nearly 90% of abusers are people the victim trusts, according to the National Center on Elder Abuse. |
Scenario 1: Collection fraud

- Terri received a call from an IRS agent.
- The man said that Terri owed back taxes and needed to pay the amount owed immediately.
- He told her that if she didn’t pay the minimum amount on the outstanding debt, the police would be sent to arrest her.
- He then said that he could accept payment over the phone via credit card or checking account.
- What would you do if you were Terri?
- Fortunately, Terri was prepared. She recognized some red flags and gave no information to the scammer.

List red flags

- 
- 
- 

Your trusted family members/friends

- 
- 
-
Scenario 2: Grandparent scam

Caller: Hi, Grandpa! It’s your favorite grandson. Can you guess which one?

Grandpa: Is this Bobby?

Caller: Yes, Grandpa! It’s Bobby. Do you remember where I go to school?

Grandpa: Of course! You go to State. How’s school?

Caller: Well, school is all right. I’m really sorry to call you about this, but I’m in a little trouble. I was at school, and some friends and I decided to drive to Mexico for spring break. We were out last night and got into a car accident. When the police searched the car, they claimed they found drugs. Now I can’t get back into the country unless I pay a fine. We’re out of cash and my ATM card won’t work down here. Can you please talk to the public defender to work this out? Please don’t tell Mom and Dad. I’m scared, Grandpa, and I just want to get back home. I’m handing the public defender the phone now.

New voice: Hello, sir. Your grandson could be in serious trouble, but I can get him and his friends out of jail if they pay a simple fine. Here is the account information where you can wire the money.

List red flags
Scenario 3: Sweetheart scam

• Let’s consider a scenario where a 78-year-old woman meets a potential romantic partner online.

• The man is an independent contractor working on an oil rig. He befriends the woman through an online chatroom, emails and private messages. They develop a seemingly close relationship.

• He tells the woman a “hard luck” story about a part breaking while he’s working and claims he won’t be compensated for his work until he pays to fix the part.

• The man says he can’t access his own funds because he’s on the ship and asks her to send money to a third party. He claims he’ll reimburse her after he receives his paycheck.

List red flags

• 
• 
• 
• 


Scenario 4: Lottery/Sweepstakes scam

• You receive a call from Publishers Clearing House (PCH) claiming you’ve won their sweepstakes and a Mercedes. All you must do is pay taxes on the winnings and tell no one until after you’ve received your prizes.

• You’re instructed to start the process of receiving your prizes by purchasing gift cards and reading the card numbers off to them.

• You’re told the next step is to mail cash via one-day courier to individuals who allegedly work for PCH in order to cover taxes and other fees.

• You’re skeptical and contact your financial advisor, who advises you to contact PCH.

• PCH confirms that they did not make this phone call and that winners never have to pay anything up front. They also advise you to check the list of winners on the PCH website to confirm that your name is not on the list.

List red flags

__________________________________________________________________________

__________________________________________________________________________

__________________________________________________________________________
Scenario 5: Social Security scam

- You receive a call from someone claiming to be with the Social Security Administration.
- The caller advises there is a problem with your Social Security number (SSN).
- The caller may ask you for your SSN for verification purposes.
- The caller may advise that your SSN was tied to money laundering or some other crime and that your benefits are in jeopardy.
- You may be told you need to pay a fee so everything can be straightened out.
- You may be asked to purchase gift cards and take a picture of the front/back and send it electronically via text or email. Or, you may be asked to send a money order or cash to someone.

List red flags
Other red flags

Identity verification.

Immediacy of request.

It doesn’t add up (part 1). If the request doesn’t make sense, chances are it isn’t legitimate.

It doesn’t add up (part 2). The payment needs to be in cash or wired to a third party.

It doesn’t add up (part 3). Statements don’t arrive, you receive a check for no apparent reason, or you’re asked to pay money to get money.

A vow of secrecy. The contact begs you not to tell anyone, especially family or friends.

Always choose multifactor authentication methods with your financial institutions and other service providers.
Protect yourself and those you love

Protect your personal information.

• Never provide personal information on the phone, through the U.S. mail or email or over the internet unless you know the request is legitimate.

• Shred financial and other personal documents before disposing of them. Many businesses offer electronic delivery, which can reduce your paper trail.

• Don’t carry your Social Security card or write your Social Security number on a check. Provide it only if absolutely necessary or ask to use another identifier. Typically, you’re required to provide your Social Security number only when dealing with a law enforcement or government agency; when opening an account with a bank, brokerage or other financial services firm, or an insurance company; when a background investigation or credit check is required while seeking employment; and when obtaining health care. Some states require a Social Security number disclosure in other cases, so always ask why your number is required.

• Maintain confidential documents in a secure location in your home.

Be cautious online

• Keep your computer security and antivirus software up to date. Don’t click on pop-up ads or links in unsolicited emails.

• Don’t use an obvious password, such as your birth date, your mother’s maiden name or the last four digits of your Social Security number.

• Always choose multifactor authentication methods with your financial institutions and other service providers.

• Never choose “trust this device” when using multifactor. It negates the purpose of having multifactor authentication.
Protect your credit information.

- Periodically inspect your credit report. The law requires the major nationwide consumer reporting companies – Equifax, Experian and TransUnion – to give you a free copy of your credit report each year if you request it. Visit AnnualCreditReport.com or call 877-322-8228 to order your free credit report each year. You also can write to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

- You can place a “fraud alert” on your credit reports. This entitles you to a free copy of your credit report and tells creditors to follow certain procedures when opening accounts in your name or making changes to your existing accounts. For an initial 90-day fraud alert, call the three credit agencies above: Equifax, Experian and TransUnion.

Be diligent with compromised accounts

- Close any accounts that have been tampered with or established fraudulently. Call the security or fraud department of each company where an account was opened or changed without your approval.

- Follow up in writing, with copies of supporting documents. Use the ID Theft Affidavit at www.ftc.gov/idtheft to support your written statement.

- File a report with law enforcement officials to help you with creditors who may want proof of the crime.

- Ask for verification that the disputed account has been closed and the fraudulent debts discharged. Keep copies of documents and records of your conversations about the theft.
Other resources available

Your state Attorney General’s office
naag.org

Federal Trade Commission (FTC)
877-382-4357
ftc.gov

Consumer Financial Protection Bureau
consumerfinance.gov

Better Business Bureau
bbb.org

The Internet Crime Complaint Center
ic3.gov

Your local law enforcement agency
(Check local listings)

Guidestar
guidestar.org

Publishers Clearing House
800-459-4724
pch.com

To place a “fraud alert” on your credit record, contact:

• Equifax: 800-525-6285
• Experian: 888-EXPERIAN (397-3742)
• TransUnion: 800-680-7289
• Annual Credit Report Request Service
  P.O. Box 105281 Atlanta, GA 30348-5281
Other resources available (cont.)

Your Edward Jones Financial Advisor and Edward Jones Fraud Investigations
edwardjones.com

If you suspect fraudulent activity or need to report a missing Edward Jones credit or debit card, please call Card Member Service immediately at the following numbers:

- Edward Jones Personal MasterCard® Credit Card: 866-874-6711
- Edward Jones Business MasterCard® Credit Card: 866-874-6712
- Edward Jones VISA® Debit Card: 888-289-6635
Scenario 1

Friend or fraud

Red flags

Next steps

Your elderly neighbor, Joe, tells you that a man knocked on his door yesterday collecting money for a food pantry. Although he can’t remember the name of the pantry, he remembers the man said he was part of the Good Neighbor Food Group. When Joe asked the man if he had a business card or any literature about the organization, the man said he would stop back by with more information. Joe asks what you think.

Friend or fraud? (circle your choice)

Were there any red flags?

________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________

What steps could you take to investigate the situation?

________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
You receive a phone call from your credit card provider’s client fraud investigation unit. The caller asks you to verify your account information, including your credit card number.

**Friend or fraud? (circle your choice)**

**Were there any red flags?**

________________________________________
________________________________________
________________________________________
________________________________________

**What steps could you take to investigate the situation?**

________________________________________
________________________________________
________________________________________
________________________________________
You receive a letter from a law firm that includes a gas bill dated six months prior and marked past due. The letter states that you are delinquent in payment and that your natural gas will be shut off in three days unless you make an immediate payment via credit card or wire to the law office. This is the first and only notice you have received and, to your knowledge, your gas bill is up to date.

Friend or fraud? (circle your choice)

Were there any red flags?

What steps could you take to investigate the situation?

______________________________

______________________________

______________________________

______________________________

______________________________

______________________________

______________________________

______________________________

______________________________