



You Have the Power to
**Outsmart the
Scammers**

Participant Workbook

Your Name: _____

edwardjones.com
Member SIPC

Edward Jones[®]
MAKING SENSE OF INVESTING

Outsmart the Scammers

Program Synopsis

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

During the program, we'll discuss how to spot certain red flags that may indicate a fraudulent encounter, resources individuals can turn to in the event they or loved ones are targeted, and steps attendees can take to help protect themselves 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

14.4
million

As many as 14.4 million Americans have their identities stolen each year, either individually or through a data breach, according to the Federal Trade Commission (FTC).

\$2.9
billion

Fraud and financial abuse schemes targeting the elderly are growing problems in the United States that cost victims at least \$2.9 billion annually, according to the Department of Justice.

1 in
10

Approximately 1 elder in 10 is victimized financially, according to the Department of Health & Human Services' National Center on Elder Abuse.

1 in
14

Only 1 case in 14 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?
- Luckily, 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 alright. 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 I got a speeding ticket. 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 wire me some money, and I can pay you back when I return? Please don't tell Mom and Dad. I messed up, but it's only a speeding ticket. I just want to get back home.

LIST RED FLAGS



Scenario 3: Sweetheart Scam

- New York authorities arrested a woman for the theft of thousands of dollars from an 85-year-old man in what experts refer to as a “sweetheart scam.”
- The two met online and developed a seemingly close relationship over a short period of time.
- The woman befriended the man by telling him “hard luck” stories, even claiming she needed money for cancer treatment.
- She persuaded him not only to give her money but also sign over his power of attorney.
- She used this to obtain a home equity loan and then stole the funds.

LIST RED FLAGS



Scenario 4: Lottery/Sweepstakes Scam

- Toni received a call from her mother, Monica, who had received a letter from the state sweepstakes commission asking her to call an 800-number to claim her cash prize.
- Monica mentioned that she didn't even recall entering a contest.
- Toni was skeptical and contacted her financial advisor, Ruth.
- Ruth advised Toni to ask Monica to contact the Federal Trade Commission.
- The FTC confirmed the state sweepstakes commission didn't exist.

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 will advise that your SSN was tied to money laundering or some other crime and that your benefits are in jeopardy.
- You will be told you need to pay a fee so everything can be straightened out.
- You may be asked to purchase gift cards and either 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 multi-factor authentication methods with your financial institutions and other service providers.

A photograph of two women walking outdoors. The woman in the foreground is older, with short white hair, wearing a blue long-sleeved shirt. She is pointing her right index finger towards the right side of the frame. Behind her and slightly to the left is a younger woman with blonde hair tied back, wearing a yellow cardigan over a grey top. They are both smiling and looking towards the right. The background is a bright, out-of-focus outdoor setting with green foliage.

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 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 anti-virus 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 multi-factor authentication methods with your financial institutions and other service providers.

Protect Yourself and Those You Love (continued)

- **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 www.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 OK.
- 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

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 (continued)

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

A photograph of an Edward Jones financial services branch at night. The building has a dark blue facade with large glass windows and doors. A prominent white sign with the "Edward Jones" logo is mounted above the entrance. To the right of the entrance, a traffic light pole stands with a red light illuminated. A "ONE WAY" street sign with an arrow pointing left is also visible on the pole. The scene is lit by streetlights and the building's own lights, creating a warm glow against the dark sky.

Edward Jones

Friend or Fraud?

SCENARIO 1

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?

Friend or Fraud?

SCENARIO 2

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?

Friend or Fraud?

SCENARIO 3

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?
