At Edward Jones, we want to empower our clients and their families to help protect themselves. We understand that confidentiality is key in any financial relationship. We also recognize that your personal and financial data contain your private information, and we are committed to keeping this information secure and confidential.

Fighting financial fraud starts with education as well as communication between family members and their financial professionals. The following information can help you recognize possible issues, prevent fraudulent activity and protect yourself or a loved one if fraud does occur.

Older Adults Can Be a Target

- According to the FBI, scam artists often seek out older Americans because:
  - They have concentrated wealth
  - They are less likely to report fraud
  - They were raised to be polite and trusting, and con men prey on these qualities
  - Mental impairment may make it difficult for them to recognize financial schemes

- Older adults, especially those who are new to the role of household decision maker, may be more prone to scam artists who demand quick decisions.

- Seniors may feel indebted to someone who has provided unsolicited advice or other assistance.

- Older victims may not report crimes because they are concerned their relatives may think they no longer have the mental capacity to take care of their own financial affairs.

- Senior women who live alone are especially vulnerable to scams: Women are nearly twice as likely to be victims of elder financial abuse as men. They may have less experience with handling financial issues and therefore may be more readily manipulated.

Facing the Facts

As our population ages, abuse of older adults will likely increase along with their numbers. Already, 17% of Americans over age 65 report that they have been “taken advantage of financially in terms of inappropriate investments, unreasonably high fees for financial services or outright fraud.”

Although elder abuse comes in many forms, elder financial abuse has been identified as the third most commonly substantiated type of crime against seniors, following neglect and emotional/psychological abuse.
### Common Types of Fraud That May Affect Mature Investors

<table>
<thead>
<tr>
<th>Type of Fraud</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Identity Theft and Phishing</strong></td>
<td>Older adults may be less “tech-savvy” than younger generations and therefore more susceptible to phishing schemes. As thieves become more sophisticated in their online approaches, seniors may find it difficult to tell whether the business requesting their personal information is legitimate. In addition, threats of closing an account or canceling a credit card may add to the victim’s insecurity and make him or her want to respond more quickly.</td>
</tr>
<tr>
<td><strong>Caregiver Fraud</strong></td>
<td>A dishonest caregiver could steal valuables or cash from the person he or she has been paid to assist. Other schemes involve intercepting the victim's mail to obtain credit card numbers and information and then using this information to commit identity theft.</td>
</tr>
<tr>
<td><strong>Romance Scam</strong></td>
<td>Email, social networking and dating websites are commonly used to start and continue relationships. Unfortunately, these channels are sometimes used to defraud individuals by exploiting their trust and vulnerability. Once a level of trust has developed, the scammer will ask the victim to send money to help get the scammer or a family member out of a difficult financial situation. Some of these online relationships may quickly develop into what appears to be a romance. Often, promises of undying love and even marriage can result.</td>
</tr>
<tr>
<td><strong>Lotteries/Sweepstakes</strong></td>
<td>An older person may receive a call, an email or a letter stating that he or she could win, or has already won, a “valuable” prize or a large amount of money. The recipient is then asked to send money to cover taxes, shipping or processing fees on the “winnings.” The prize may never be delivered, or, if so, is usually worth less than the money paid to retrieve it. In many instances, lottery scams involve foreign countries or individuals calling from long distances.</td>
</tr>
<tr>
<td><strong>Grandparent Scams</strong></td>
<td>A caller may claim to be a grandchild (or another relative or a friend) who needs money. If the recipient responds with a grandchild’s name, the caller can use this information to convince the recipient the call is legitimate. The thief may employ any number of scenarios to gain sympathy and money; a common tale involves an arrest or auto accident while in another country. More elaborate scams have included an “attorney” or a “public defender” to validate the story and emphasize the urgency of the situation. The thief may also plead with the recipient not to tell his or her parents.</td>
</tr>
<tr>
<td><strong>Social Security Scams</strong></td>
<td>An individual will receive a call, allegedly from the Social Security Administration, notifying them there is an issue with their Social Security number (SSN), and they need to call back at a number provided or their benefits will be stopped. When the person calls back, they speak to an “officer” with the administration, who requests them to verify their name and SSN. They will then be told their SSN has been tied to or used in a serious crime, and they could face charges, along with their benefits being suspended. They will typically be instructed to purchase prepaid money cards in order to alleviate the situation. The method of payment can escalate into other forms of payments at higher amounts, even when the person complies.</td>
</tr>
</tbody>
</table>

### Red Flags

The following red flags may indicate financial exploitation of an older adult:

- A rapid decline in the value of the victim’s account
- Withdrawals from the victim’s account that are inconsistent with previous spending habits
- Essential bills going unpaid, despite adequate income
- Missed appointments
- Acquaintances or family members who seem overly interested in an older adult’s finances
- Concern or confusion about missing funds from an account
- Unexplained changes in beneficiary designations
- A sudden, close relationship with a new “friend”
- Statements sent to an address other than that of the victim
- Missing belongings or property
- A caregiver who isolates the older person from family, friends, community and other stable relationships
- The need to send money in order to receive a windfall (e.g., lottery winnings, estate settlements, etc.)
- The need to send additional money after an initial payment has been made
# How to Help Combat Financial Fraud

<table>
<thead>
<tr>
<th>Investigate before Investing</th>
<th>Know the Fears Con Artists Prey Upon</th>
<th>Be Wary of Unsolicited Offers</th>
<th>Protect Personal Information</th>
</tr>
</thead>
</table>
| • Take the time to conduct research. Asking a promoter for more information or for references is not enough because thieves have no incentive to give accurate information.  
• Talk to family or friends before making an important decision regarding finances.  
• Understand the investment, the risks and the company’s history. | Many older investors worry about the adequacy of their retirement savings, especially if they are faced with costly medical expenses. Con artists may pitch their schemes as a way to increase financial security, but only if the older adult acts immediately. | • Thieves use email, faxes and internet postings to create a buying frenzy to boost the share price of thinly traded stocks. Once they quit promoting the company, the share price quickly falls.  
• If the victim sends money abroad and something goes wrong, the funds are more difficult to trace and nearly impossible to recover. | • Shred financial documents and paperwork with personal information before you discard them. Many companies, including Edward Jones, offer electronic delivery, which can help reduce a paper trail.  
• Protect Social Security numbers. No one should carry a Social Security card in his or her wallet or write a Social Security number on a check. Give this number out only if absolutely necessary or ask to use another identifier.  
• No one should give out personal information over the phone, through the mail or over the internet unless he or she knows the recipient is legitimate.  
• Thieves can use links in unsolicited emails to take advantage of older adults. Instead, type in a web address you know. Firewalls, anti-spyware and anti-virus software can help protect a home computer, especially if they are kept up to date.  
• Be alert if the older adult experiences any of the following, which require immediate attention:  
  - Bills that do not arrive as expected  
  - Unexpected credit cards or account statements  
  - Denials of credit for no apparent reason  
  - Calls or letters about purchases he or she did not make  
• Credit reports contain information about a person’s accounts and bill-paying history. The law requires the major nationwide consumer reporting companies to give each American a free copy of his or her credit report on request once per year. |
If Fraud Occurs:

• Placing a “fraud alert” on a credit report entitles the person to a free copy of his or her credit report and tells creditors to follow certain procedures when opening accounts in that person’s name or making changes to existing accounts. For an initial 90-day fraud alert, call one of the following:
  – Equifax: 866-349-5191
  – Experian: 888-EXPERIAN (397-3742)
  – TransUnion: 800-680-7289
• Keep copies of documents and records of conversations about any theft.
• File a complaint with the Federal Trade Commission at 877-ID-THEFT (438-4338). The FTC maintains a database of identity theft cases used by law enforcement agencies for investigations. You can also file a complaint online at ftc.gov/complaint.
• If theft of mail occurred, contact the U.S. Postal Inspection Service at 877-876-2455.
• Contact the Social Security Administration’s Fraud Hotline at 800-269-0271 if a Social Security number has been used fraudulently.

Additional Resources

• edwardjones.com/privacy
• Federal Trade Commission [ftc.gov; 877-FTC-HELP (382-4357)]
• Identity Theft Resource Center (idtheftcenter.org)
• National Consumers League (nclnet.org)
• U.S. Postal Service (usps.com)
• Federal Bureau of Investigation – Be Crime Smart (fbi.gov/scams-and-safety)
• FINRA Scam Meter (tools.finra.org/scam_meter/)
• Securities and Exchange Commission – Investor Alerts and Bulletins (sec.gov/investor/alerts.shtml)
• Federal Bureau of Investigation Internet Crime Complaint Center (IC3) (ic3.gov/default.aspx)
• AnnualCreditReport.com (annualcreditreport.com; 877-322-8228)
• identitytheft.gov

1 The MetLife Study of Elder Financial Abuse, Mature Market Institute, 2011
2 Investor Protection Trust Survey, 2016