Fraud and the Older Adult

Each year, thousands of people living in America unwittingly fall victim to marketing fraud and identity theft scams. Congress estimates that consumers lose billions annually to telemarketing fraud alone. According to the National Consumers League (NCL), older adults are being increasingly targeted by scammers. In 2010, older consumers made up 54% of all NCL complaints, a 5.5% rise over the previous year. Alarmingly, the number of incidents reported by consumers age 65 and older have increased by nearly 6% since 2009.

Older adults are targeted for crimes for several reasons:

- **Availability:** Older adults are often home for cold calls and scam artists. Also, older adults increasingly use email and the Internet, the most popular venues for scammers.
- **Isolation:** Very often, older adults do not live near family and have nobody to review financial and investment decisions.
- **Loneliness:** Lack of friendships can position some to be receptive to the friendly voice of a con artist.
- **Health Issues:** As one ages, natural health issues evolve. Disabilities leave older adults unable to repair and upkeep homes, positioning them for scams and fraud.
- **Money:** Older adults are often targeted because cons see them as trusting and easy targets for theft of money from savings or property.

How Marketing Scams Work

How'd they find me? Fraudsters get contact information from many sources. Some purchase mailing lists or use special software to trawl the Internet for email addresses. Telemarketers may refer to the local phonebook, purchase lists of those who have responded to previous solicitations, or use an automated program to dial random numbers sequentially. A fraudulent telemarketing operation is usually a "boiler room," where seasoned operators try to scam people. Common scam mediums include:

- **Email and Internet:** Using fake email addresses with links to websites that claim to be from a financial institution or government agency, "phishers" fool you into divulging your Social Security number, PIN, credit card number, or other personal information.

- **Cold Calls:** Telemarketing scammers may call with bogus product offers or request donations to a fake charity. "Bank representatives" who call to warn you of an account breach and "market researchers" who ask you to participate in a survey may actually be phishers trying to steal your financial data.

- **Text Message:** Claiming to be old friends or admirers, text scammers tempt you into replying. Return calls are redirected to a premium-rate service without your knowledge, and you are charged a high per-minute fee.

- **Direct Mail:** You receive mail saying you've won a prize or a contest. The instructions tell you to respond with certain information. If you do, you'll be contacted by a fraudster.

- **Online, Broadcast, and Print Ads:** You click, call, or write in response to an advertisement. The fact that you initiate the communication doesn't mean the business is legitimate.

Warning Signs of Fraud

- "Free" gifts that require you to pay shipping and handling, redemption fees, or tax before delivery.
- "High-profit, no-risk" investments.
- "Act now" and other high-pressure sales tactics.
- A request for a credit card, bank account, or Social Security number to verify that you have won a prize.
- Refusal to provide basic written information about an organization.
- Organizations that are unfamiliar or have no physical address (i.e., those with only a post office box or Internet address).

Social Media Fraud: A Growing Concern

The popularity of social networking sites such as Facebook has caught the attention of fraudsters. According to Scambusters.org, the current top five social media scams involve using a false identity to commit fraud, malware (links that, when clicked, upload spyware, trojans, or viruses to your computer), profile hacking, identity theft, and spam.

How to Combat Fraud

- Don't be pressured to make a quick decision.
- Never give out your bank account, credit card, or Social Security numbers unless you know the request is legitimate.
- Avoid posting your email or home address or phone number on unsecure Internet sites.
- Scrutinize email carefully. Never click on a link unless you know it is from a reliable source. Delete spam without opening.
- Be wary of responding to unknown calls/texts from unfamiliar or foreign area codes.
- Use privacy settings on social media sites to control access to your profile.
- Keep your computer safer by installing a firewall, updating your operating system with
- the latest security patches, and using current antivirus software.
- Be wary of statements that you've won a "prize." Don't agree to pay a fee to receive it.
- Before giving, check out the charity with the Better Business Bureau (BBB). Check out all unsolicited offers with the BBB, local consumer protection agency, or state attorney general's office.
- When hiring a contractor, select only a licensed professional. Always insist on a written contract or financial agreement—and read carefully before signing.
- Don't pay in full for a home improvement or other service if asked for a deposit.
- Beware of offers to "help" you recover lost money or improve your credit. If you are having financial difficulties, consult a nonprofit consumer credit counseling service or work directly with your mortgage lender, credit card company, or other lender/service provider.
- Cons often take advantage of consumer goodwill after disasters such as floods and earthquakes. Check out relief organizations with the BBB before donating.
- Use gift cards and gift certificates promptly. If a company closes or goes bankrupt, it may be impossible to get refunds for the unused balance. Note that federal rules limiting the fees card issuers may charge took effect in 2010.
- Forward unsolicited email to spam@uce.gov. Messages are stored in a database for law enforcement agencies to use in their investigations.
- List your phone number on the National Do Not Call Registry to reduce the number of telemarketing calls you receive.

Fraud Facts

In 2010, 38% of all fraud complaints were made by people age 50 and over. (Federal Trade Commission, *Consumer Sentinel Network,* March 2011)

Consumers reported more than $3.6 million in losses to the NCL Fraud Center in 2010. The average loss per person to Internet scams alone was $931. ("Mid-year report: Internet merchandise scams topping complaints to NCL's Fraud Center," 2010)

The top three categories in the 2009 Consumer Complaint Survey Report were 1. auto (false advertising, faulty repairs, towing disputes), 2. credit/debt (billing disputes, mortgage fraud, credit repair and debt relief services, predatory lending, illegal debt collection tactics), and 3. home improvement/construction (shoddy work, failure to start or complete the job). (Consumer Federation of America, 2010)

The Internet is the choice venue of con artists. Among the top web-based scams reported in 2010 were sales of merchandise not delivered or misrepresented (37.4%), fake checks (31.3%), prize/sweepstakes/free gift offers (10.5%) phishing/spoofing (7.2%), and advance fee loans/credit arrangers (2.9%). Other Internet scams included phishing, advance fee loans/credit assistance, Nigerian money offers, "sweetheart swindles," employment/job counseling, and bogus business opportunities. (National Consumers League, "Top Scams of 2010")

Top telemarketing fraud schemes involved prizes/sweepstakes/gifts (40%), fake checks (26%), and phishing/spoofing (12%). Telemarketing scams included timeshare resales, magazine offers, advance fee loans/credit arrangers, and scholarships/grants. (National Consumers League, "Top Scams of 2010")

Fraudsters haven't abandoned the telephone as a method of contact. In 2010, 23.6%—up more than 7% over the previous year—of victims reported being defrauded over the phone. (National Consumers League, "Top Scams of 2010")

Despite government regulation, the amount of unsolicited bulk email, commonly known as "spam," accounts for more than 80% of all messages received. (Symantec, "The State of Spam: A Monthly Report," January 2011)

The Consumer Sentinel Network, a fraud complaint database developed and maintained by the Federal Trade Commission, received 1.3 million consumer fraud and identity theft complaints in 2009. (Federal Trade Commission, *Consumer Sentinel Network Data Book for January – December 2009*, February 2010)

Economic downturn has led to a rise in securities and commodities fraud (e.g., pyramid and Ponzi schemes, advance fee fraud, high-yield investment fraud). Over the past five years, investigations into these types of schemes have increased by 33%, while associated losses total billions of dollars. (Federal Bureau of Investigation, *2009 Financial Crimes Report*)

Resources

Better Business Bureau
www.bbb.org

Credit Bureaus

Annual Credit Report Request Service
(877) 322-8228
www.annualcreditreport.com

OptOutPrescreen.com
(888) 567-8688 (5OPTOUT)
TDD: Call 711 and refer the relay operator to (800) 821-9631
www.optoutprescreen.com

Experian (formerly TRW)
(888) 397-3742 (Experian)
(to order credit report and to report credit card fraud)
www.experian.com

Equifax
(888) 766-0008 (to report credit card fraud)
(800) 685-1111 (to request credit report)
www.equifax.com

TransUnion
(800) 680-7289 (fraud victim assistance)
(800) 877-322-8228 (to request credit report)
www.transunion.com

Consumer Federation of America
1620 I Street NW, Suite 200
Washington, DC 20006
(202) 387-6121
www.consumerfed.org

Direct Marketing Association
(to remove your name from direct mail, telemarketing, and email lists)
www.the-dma.org

Electronic Crimes Task Force
www.ectaskforce.org

Federal Bureau of Investigation
www.fbi.gov

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) 382-4357 (FTC-HELP)
(877) 438-4338 (ID-THEFT)
consumeralerts@fdic.gov
www.ftc.gov/bcp/index.shtml
www.consumer.gov/idtheft

Identity Theft Prevention and Survival
www.identitytheft.org

Internet Crime Complaint Center
(to report Internet crimes)
www.ic3.gov

Internet Fraud Watch
(800) 876-7060
www.fraud.org

National Consumers League Fraud Center
(to report suspected Internet or telemarketing fraud)
(800) 876-7060
www.fraud.org

National Cyber Security Alliance
1101 Pennsylvania Avenue, NW, Suite 600
Washington, DC 20004
www.staysafeonline.org

National Do Not Call Registry
(to remove your name from
telemarketing call lists)
www.donotcall.gov

Privacy Rights Clearinghouse
3100 – 5th Avenue, Suite B
San Diego, CA 92103
(619) 298-3396
www.privacyrights.org

U.S. Department of Justice Disaster Fraud Hotline
(to report disaster-related fraud)
(866) 720-5721
disaster@leo.gov
www.usdoj.gov

United States Postal Inspection Service
Attn.: Mail Fraud
222 S Riverside Plaza, Suite 1250
Chicago, IL 60606-6100
(877) 876-2455
https://postalinspectors.uspis.gov/

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) 382-4357 (FTC-HELP)
(877) 438-4338 (ID-THEFT)
consumeralerts@fdic.gov
www.ftc.gov/bcp/index.shtml
www.consumer.gov/idtheft

Identity Theft Prevention and Survival
www.identitytheft.org

Internet Crime Complaint Center
(to report Internet crimes)
www.ic3.gov

Internet Fraud Watch
(800) 876-7060
www.fraud.org

National Consumers League Fraud Center
(to report suspected Internet
or telemarketing fraud)
(800) 876-7060
http://bit.ly/bfvVQl

National Cyber Security Alliance
1101 Pennsylvania Avenue, NW, Suite 600
Washington, DC 20004
www.staysafeonline.org

National Do Not Call Registry
(to remove your name from
telemarketing call lists)
www.donotcall.gov

Privacy Rights Clearinghouse
3100 – 5th Avenue, Suite B
San Diego, CA 92103
(619) 298-3396
www.privacyrights.org

U.S. Department of Justice Disaster Fraud Hotline
(to report disaster-related fraud)
(866) 720-5721
disaster@leo.gov
www.usdoj.gov

United States Postal Inspection Service
Attn.: Mail Fraud
222 S Riverside Plaza, Suite 1250
Chicago, IL 60606-6100
(877) 876-2455
https://postalinspectors.uspis.gov/