



Scam Prevention Project

Included in this packet:

- Most common scams
- Most common Medicare scams
- Most common internet scams
- Examples of mail scams
- Scam Action Plan
- Scam prevention quiz
- Scam red flags
- Prevention tips
- Quiz answer key

Materials prepared by the East Bay Community Law Center

For questions, or if you suspect you have been victim of a scam, please call your local legal services provider.

MOST COMMON SCAMS



Sweepstakes/ lottery scam

Fraudsters send seniors a check they have “won,” and the senior advances the fraudsters fees before the check bounces.



Romance scam

Scammers create fake online profiles using photos of other people, they profess their love quickly and tug at your heartstrings with made-up stories of how they need money.



Door-to-door scams

Fraudsters come to your door, offering to install solar panels, pave a driveway, or lower bills. Fraudsters refuse to give details or let you review a contract.



Medicare/ health insurance scams

Scammers may pose as a Medicare representative to get older people to give them their personal information, then use the personal information they provide to bill Medicare and pocket the money.



Funeral and cemetery scams

Fraudsters read obituaries or attend funerals of someone they don’t know, and then call the widow claiming the deceased had a debt with them. Disreputable funeral homes tack on extra charges onto funerals.



Telemarketing/ phone scams

Scammers solicit money for a fake charity. Scammers get older people to wire over transaction fees for large inheritances or money they have “found” for the senior. Scammers call seniors repeatedly.



Internet fraud

Fraudsters fool victims into downloading a fake anti-virus program through a pop-up window. Seniors receive an email from a seemingly legitimate company asking them to update their information with the IRS.



Homeowner/ mortgage

Scammers advertise on telephone poles and via flyers. Scammers request an upfront fee for loan modification and offer to make payments to a company other than your lender.



Identity theft



Fraudsters get your personal information and runs up bills in your name. You find out by checking your bank statements or your credit report, or getting bills for something you didn’t authorize.



Grandparent scam

Scammers call and claim your grandchild is in trouble and needs help with an emergency, such as getting out of jail, paying a hospital bill, or leaving a foreign country.

MOST COMMON MEDICARE SCAMS

	Billing for services or items not needed	Fraudsters will send bills for medical tests or equipment that is not needed, or send bills for services that Medicare provides for free so they can steal Medicare numbers.
	Upcoding	Scammers will bill Medicare for a more expensive procedure than what was given. For example, a toenail trimming could be exaggerated and labeled as a surgical procedure.
	Marketing violations	Fraudsters can come to your door trying to sell something, misrepresent a service, or call on the phone asking for personal information.
	Solicitation of Medicare Beneficiaries	Scammers can offer bribes, gifts or free rides in exchange for Medicare numbers.
	Ambulance Fraud	Fraudsters falsify documentation to bill for more miles than were actually driven or for different services than what were provided, for example a false medical necessity or labeling a non-emergency as a medical emergency and billing as such.
	Durable Medical Equipment	Scammers will not follow marketing rules for Medicare-covered items, for example contacting someone who has not given written permission to be contacted.
	Home Health Services Fraud	Fraudsters ask beneficiaries to sign forms that verify a nurse or therapist has come to their home and provided services. A physician may falsely certify that the beneficiary is an insulin-dependent diabetic and cannot inject himself.
	Part D Fraud	Scammers will send bills for medication that was not provided, bill for "ghost patients," forge physician signatures on prescriptions, or overprescribe medications.

MOST COMMON INTERNET SCAMS

	Phishing scam	Scammers will send you messages via email or social network to try to obtain login credentials from your bank account, social network, work account or gain access to any other valuable personal data.
	Money laundering scam	Scammers may send emails that appear to contain an emotional message from an official government member, a businessperson or a very wealthy family member. The message will ask you to pay some initially small fees for paper and legal matters.
	Greeting card scam	You may receive greeting cards in your email inbox that appear to be coming from a friend. Clicking on the card usually ends up with malicious software downloaded and installed onto your computer.
	Fake antivirus software	While browsing the Web, a pop-up message appears on your screen claiming your computer has been infected by a virus. You may be invited to download a program to scan your computer for viruses and pay a fee. This will result in an unnecessary loss of money and/or an installation of malware.
	Travel scam	Scammers send emails containing an exclusive, limited time offer to an exotic location. They may hide necessary costs until you pay the initial offer, or others may just take your money without sending you anywhere.
	Guaranteed bank loan or credit card scam	An email may offer a pre-approved loan or credit card from the bank. In order to receive the sum or the loan, the bank will require you to pay an annual fee up front.
	Hitman scam	Scammers will send threatening emails in order to extort money from their victims. The scammer might threaten to hurt you unless you pay a large sum, or threaten to kidnap a family member unless a ransom is paid within a certain period.
	Hijacked profile scam	Social media networks can be hijacked without taking precautionary measures. Log in credentials, personal data and passwords should be carefully protected.
	Easy money or economic scam	Scammers will offer you easy money on the Internet through work-at-home jobs, plans and methods of getting rich quickly or money from a government source.
	Charity scam	In the aftermath of a disaster, scammers may send emails seeking money for victims. Instead of contributing through the link that may be provided through the email, donate directly to a trusted website or charity that you know.

The following are examples of scams seniors have received in the mail.



REMEMBER:

- **Receive a free copy of your credit report**

Check your credit report annually, at no charge, by visiting www.annualcreditreport.com. Be sure to request the report include all three major credit reporting agencies – Equifax, Experian and TransUnion.

- **Stop junk mail**

For removal from most national advertising mailing lists, register at www.dmaconsumers.org (\$1 fee) or send your name and home address, along with a check or money order, payable to IMS, for \$1 to Attn: IMS, Mail Preference Service (MPS), P.O. Box 643, Carmel, NY 10512-0643.

- **Stop pre-approved credit card offers**

The credit bureaus offer a toll-free number that enables you to “opt-out” of having pre-approved credit offers sent to you for five years. Call (888) 567-8688 or visit www.optoutprescreen.com for more information.

- **Stop telemarketing calls**

The federal government has created the National Do Not Call Registry – a free easy way to reduce the telemarketing calls you get at home. To register your phone number or to get information about the registry, visit www.donotcall.gov or call (888) 382-1222 from the phone number you want to register.

- **Check to be certain a company offering home improvement services is properly licensed before you do business.**

DELIVERY DIRECTIONS
IDENTIFIED INDIVIDUAL

Address _____
City _____ State _____ Zip _____

PLEASE DELIVER THIS PARCEL WITH CONTENTS AS ADDRESSED. THIS IS BEING
RECEIVED FROM KNOWN INDIVIDUAL



EXPECTED MAIL: THIS ENVELOPE IS EXPECTED IN OUR MAIN OFFICE.

PI
CO
PO
H

- - EXPECTED MAIL - -
**PROCEED IMMEDIATELY WHEN
RECEIVED**

SEAT BELTS SAVE LIVES. BUCKLE UP!

MOTOR VEHICLE / AWARD REGISTRATION

Department of Distribution, Regional Office
Financial & Property Awards
PMB 293, 1153 LEE ST.
DES PLAINES, IL 60016-6503

HMA CRE-17-17



**DIRECTIVE
CONFIRMATION FORM**

FOR IMMEDIATE DOCUMENT RELEASE:

\$2,353,226.31

REFERENCE ID NO. 10022191055

ISSUED EXCLUSIVELY TO:

[Redacted Name]

MAIL NOW TO: Payment Documentation Director
PO BOX 6427
Fort Lauderdale, FL 33310-6427



USPS-001 1000

I, [Redacted] confirm my
identity and accept my \$2,353,226.31 opportunity status.

I have NOT collected more than \$50,000.00 in prize winnings
before.

I have enclosed \$20 processing stipend payable to P.I.S. for
immediate Priority Delivery of \$2,353,226.31
prize payout data release.

Sworn and affirmed by: [Redacted]

X _____

IMPORTANT INSTRUCTIONS

We are trying to reach you regarding your \$2,100,000.00 Sweepstakes ID
printed to the right. Upon legal entry and eligibility verification, prize will
be awarded to the selected winner as 30 annual installments of \$70,000.00.
Call the number imprinted below your code to complete the entry process.

ENTRY CODE NO. 724379619

CALL

1-800-687-9411

NME PRIZE DISBURSEMENT
16120 US HIGHWAY 19N
CLEARWATER, FL 33764

The
Sum of: Two Million One Hundred Thousand Dollars and xx/100

\$2,100,000.00

Entry is hereby granted to:

*****AUTO**SCH 5-DIGIT 94601
724379619

KEEP FOR YOUR RECORDS



Eric Marshall
Attorney at Law

AO 93 (Rev.12/09) Arrest Warrant

UNITED STATES DISTRICT COURT

In the Matter of Arrest For,
NON-PAID LOAN AND CHECK FRAUD

Case Number: -FL 073/2015/3648

ARREST WARRANT

To: - Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requested to arrest the following person.

Charges Pressed against the name are:-

Count 1: Violation of federal banking regulation

Count 2: Collateral Cheque Fraud (According to act no 76)

Count 3: Theft By The deception (According to act no 48)

PS: If you fail Respond within 48 hours this Legal Action will be activated. You be Entitled for an OOCR, so Please Reply me and listed this document.

I find that the affidavit (S) or any recorded testimony, establish probable cause to arrest the person.



(JUDGE'S SIGNATURE)
Eric Marshall

Scam Prevention Workshop Quiz

1. One way to tell whether a website offers security to help protect your sensitive data is:
 - a. The security certificate for the site matches the name of the site
 - b. Your friends shop on the website all the time and never have a problem.
 - c. You heard about the website through an online search engine.
2. What is the best way to verify if a charity that contacts you by phone or by mail is real?
 - a. Ask the charity to give you a description of what they do.
 - b. Send a donation and see if the charity gives you a receipt.
 - c. Check that the charity is trustworthy by searching for the charity online or calling their headquarters.
 - d. Assume that charities have the best intention in mind and send cash.
3. How does the Internal Revenue Service (IRS) contact people?
 - a. By calling people.
 - b. By sending people text messages.
 - c. By sending people letters.
 - d. By sending people emails with personal information included.
4. If you suspect you've been a victim of a scam...
 - a. You should report the scam to your local police station.
 - b. You should consult someone you trust, including an attorney.
 - c. You should contact Adult Protective Services.
 - d. All of the above
5. The usual suspects who might want to scam me include:
 - a. Strangers
 - b. Family members
 - c. Caregivers
 - d. All of the above
6. I receive a check in the mail, with a letter saying that I am receiving funds from an inheritance from a long-lost relative. The letter instructs me to deposit the check and wire \$500 of the funds for transaction fees. What should I do?
 - a. Consult a trusted family member or friend.
 - b. Deposit the check.
 - c. Call the phone number on the letter to make sure that the company is real.

- d. Deposit the check and wire the money.
7. Your credit report may suggest that you've been a victim of identity theft if it shows:
- a. You have a credit card, loan, or lease in your name that you know you don't have.
 - b. A company you have never heard of requested a copy of your credit report.
 - c. A home address for you that you never had.
 - d. All of the above.
8. Navigating public benefits and retirement benefits can be tricky. What is the best way to manage the complicated benefits systems?
- a. Log on to Benefits.Gov to make sure you are getting the benefits you need.
 - b. Attend a paid-for lunch to learn about how to maximize your benefits.
 - c. Answer a call from the government about your health insurance and provide your social security number so they can provide insurance discounts.
 - d. Sign up for a government-run program that will pay your bills for an up-front processing fee.
9. Which of the following is **NOT** a way to protect yourself from mortgage relief fraud?
- a. Wait to pay any money until you receive a written offer for loan modification.
 - b. Make direct payments to the mortgage relief company, rather than your lender.
 - c. Contact your lender directly if you are having trouble paying your mortgage. You may be able to negotiate a new repayment schedule.
10. Why are seniors targeted for scams?
- a. Fraudsters believe that older adults are more likely to be trusting and make small talk with strangers.
 - b. Fraudsters target older adults because they are less likely to report crimes. Some elderly victims feel embarrassed that they have fallen for a scam and others fear that family members will think they are unfit to manage their own finances.
 - c. Fraudsters believe that older adults have more difficult navigating technology.
 - d. All of the above.



My Scam Action Plan

When I am not sure if something is a scam or not, I will contact:

1. _____
2. _____
3. _____

I can also contact:

- Adult Protective Services
- My bank: _____
- My local Department of Consumer Affairs
- I can make a report with the Federal Trade Commission by going to www.ftc.gov or by calling 1-877-FTC-HELP (1-877-382-4357)
- The Consumer Financial Protections Bureau to make a complaint about homeowner fraud, scammy debt collection practices, issues with money transfers: <https://www.consumerfinance.gov/complaint/>
- The Center for Medicaid and Medicare if I suspect I am a victim of Medicaid/Medicare fraud: (1-800-447-8477)
- www.Identitytheft.gov if I suspect identity theft

RED FLAGS: Stop! It's a Scam!!

- 🚩 A **PROMISE** that you can win money, make money, or borrow money easily;
- 🚩 An **INSISTENCE** that you keep the offer secret, and not tell family or friends;
- 🚩 A **DEMAND** that you act immediately or else miss out on this great opportunity;
- 🚩 A **REFUSAL** to send you written information before you agree to buy or donate;
- 🚩 An **ATTEMPT** to scare you into buying something;
- 🚩 An **INSISTENCE** that you wire money, pay cash, or pay in iTunes or other gift cards;
- 🚩 A **REFUSAL** to stop calling after you've asked not to be called again;
- 🚩 A **THREAT** that you will go to jail or be deported;
- 🚩 An **UNPROFESSIONAL** letter with spelling and grammar errors.

SCAM PREVENTION TIPS

Ask someone: run offers and deals by people you trust, including lawyers, to see if they are legitimate.

Don't answer the phone if you don't recognize the number. If it's someone who needs to talk to you, they will leave a message.

Reach out: get involved in your community. Call a friend. Talk to your neighbors.

Don't wire money for any reason, unless you know for sure that your family or friend is abroad and needs it.

Don't use public Wi-Fi to check sensitive financial information, or to make purchases on your credit card.

Check your statements including credit card and Medicare statements to ensure that there are no unauthorized charges.

Get all offers in writing and check with someone you trust before signing contracts. If offers seem "too good to be true," they probably are.

Don't assume that because the bank accepted a check, the check is not fraudulent.

Answer Key

1. The correct answer is A. The safest way to make sure that the website is secure is to examine the security certificate. Relying upon word-of-mouth is not as effective.
2. The correct answer is C. Hanging up the phone and searching for the charity will help you determine if it is a real charity, or if it is a scam. You can also call the charity headquarters and verify that you spoke with someone from their organization. Frequently, fraudsters call with a “Firefighter Donation” scam.
3. The correct answer is C. The IRS will never contact you by phone, by text message, or by email with your personal information. If you are contacted by those means, it is a scam. You can follow up with the IRS directly. Call 1-800-366-4484 to determine if the caller is an IRS employee with a legitimate need to contact you.
4. The correct answer is D. Protect yourself and your options by reaching out to Adult Protective Services, someone you trust (including a lawyer), and the police station.
5. The correct answer is D. Although it seems intuitive that a stranger may be the one to run a scam it is often those who can easily gain someone’s trust.
6. The correct answer is A. You need to consult someone you trust, before contacting the so-called company or sending money to someone you don’t know. Always remember: even if a bank accepts a check, the check could still be fraudulent and you could be on the hook for the bounced amount.
7. The correct answer is D. Information on a credit report that you have not heard of might indicate identity theft.
8. The correct answer is A. The US Government runs a benefits navigator website that can help you figure out if you are getting the benefits you can receive. Do NOT attend a paid-for lunch to learn more about your benefits; that is a well-known scam. Do NOT sign up for a government-run program that will pay your bills for an up-front processing fee; there is no such thing. Lastly, never provide your social security number over the phone to someone claiming to be the government.
9. The correct answer is B. You want to make sure you keep paying your lender, especially if you don’t know if you can trust a mortgage relief company yet.
10. The correct answer is D. Fraudsters target elderly people because they are often more trusting, may feel shame about being scammed, and are seen as not knowing how to use technology.