

# Preventing Elder Financial Exploitation: Trends, Tips & Tools

CFPB Office for Older Americans



# Disclaimer

---

*This presentation is being made by a Consumer Financial Protection Bureau representative on behalf of the Bureau. It does not constitute legal interpretation, guidance or advice of the Consumer Financial Protection Bureau. Any opinions or views stated by the presenter are the presenter's own and may not represent the Bureau's views.*

# The Bureau's Mission and Vision

---

## **MISSION**

To regulate the offering and provision of consumer financial products or services under the Federal consumer financial laws and to educate and empower consumers to make better informed financial decisions.

---

## **VISION**

Free, innovative, competitive, and transparent consumer finance markets where the rights of all parties are protected by the rule of law and where consumers are free to choose the products and services that best fit their individual needs.

# Office for Older Americans

---

The Office for Older Americans (OA) develops initiatives, tools, and resources to:

- help protect older consumers from financial harm
- help older consumers make sound financial decisions as they age

# What is elder financial exploitation?

---

- Fraudulent or otherwise illegal, unauthorized, or improper act or process of an individual that uses the resources of an older person for personal benefit, profit or gain
- Actions that result in depriving an older person of rightful access to, or use of benefits, resources, belongings, or assets

# Examples of financial exploitation

---



Exploitation by an agent under a POA or person in another fiduciary relationship



Investment fraud and scams



Theft of money or property by family members, caregivers, or in-home helpers



Lottery and sweepstakes scams

# Who is at risk?

---

- Anyone can be the victim of financial exploitation.
- Elder financial exploitation crosses all social, educational, and economic boundaries.

# Why are some older adults at risk?

---

- Regular income and accumulated assets
- Trusting and polite
- Lonely and socially isolated
- Reluctant to report exploitation by a family member, caregiver, or someone they depend on





# Who could be the abuser?

---

- People known to person
  - Family members and caregivers
  - Friends, neighbors
  - Agents under a power of attorney
  - Financial professionals
- Strangers
  - Scammers of all types

# Why don't some older adults report financial exploitation or abuse?

---

- Shame and embarrassment
- Loyalty to family member or caregiver
- Fear of retaliation or not being believed
- Fear of being declared incompetent and placed in a nursing home
- Dependence on the abuser
- Denial or self-blame
- Lack of awareness

# How to spot potential financial abuse

---

Look out for these common signs:

- The person says money or property is missing.
- The person is afraid or seems afraid of a relative, caregiver, or friend.
- The person is reluctant to have visitors or take phone calls.
- You notice sudden changes in the person's spending or savings.

# What you can do to help

---

## **Adult Protective Services**

For elder abuse, contact Adult Protective Services.

Find contact information [eldercare.acl.gov](https://eldercare.acl.gov) or call 1-800-677-1116.



Consumer Financial  
Protection Bureau

# What you can do to help

---

## **Local Police - 911**

If someone is in danger or a crime has been committed, call the police.

## **Your State Attorney General**

Visit [naag.org](http://naag.org) to find yours.

# What you can do to help

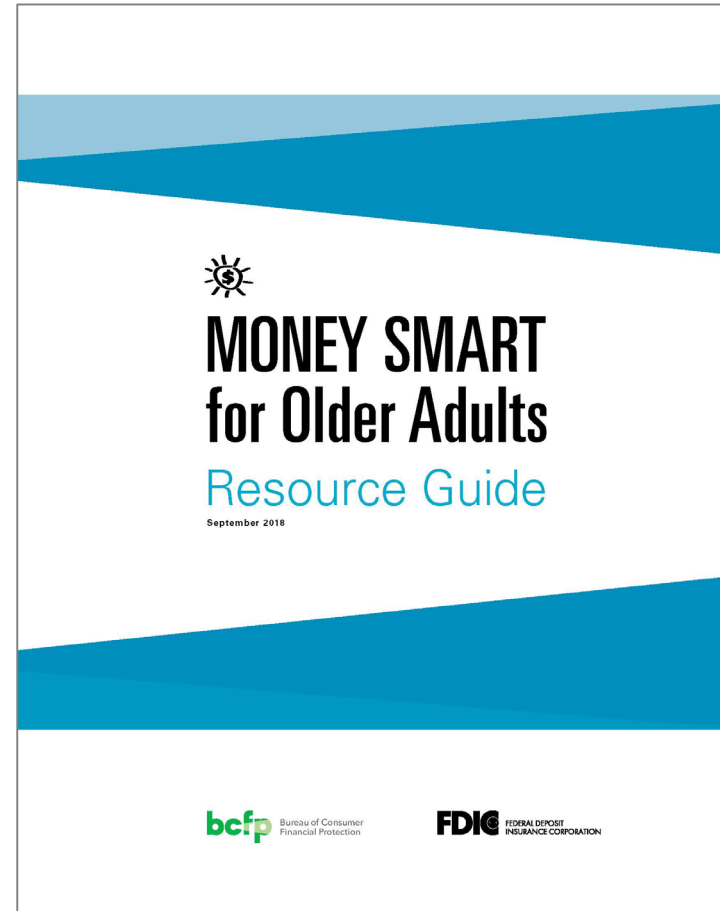
---

- Submit scams to the FTC at [ftc.gov/complaint](https://ftc.gov/complaint)
- Report mail fraud to the U.S. Postal Inspection Service at [usps.gov](https://usps.gov).

# Money Smart for Older Adults

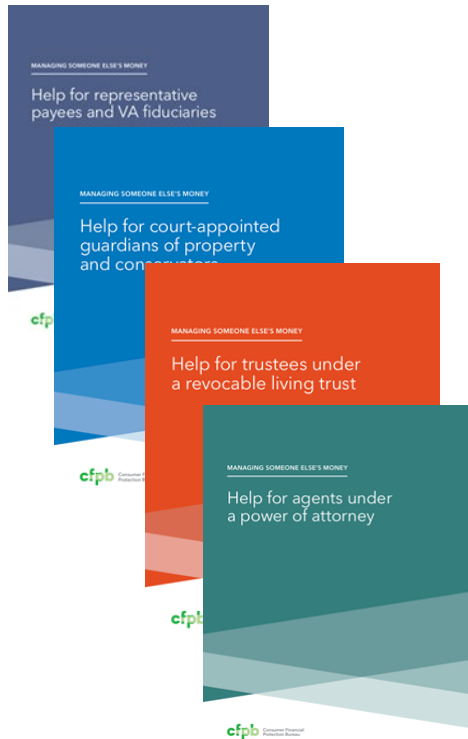
---

- An awareness program developed in collaboration with the FDIC
- Identify scams, fraud and other forms of exploitation
- Instructor guides available for download
- Resource guide available in bulk at no charge
- Available in English and Spanish



# Managing Someone Else's Money

---



- Help for financial caregivers handling the finances for a family member or friend who is incapacitated
- Guides for four common types of financial caregivers:
  - Agents under a Power of attorney
  - Guardians and conservators
  - Trustees
  - Social Security and Department of Veterans Affairs (VA) representatives
- Includes tips on protecting assets from fraud and scams.
- Available in English and Spanish



# Tips and advice for older consumers

---

## Consumer advisories:

- Share financial information with your spouse now to avoid problems later
- Co-signing student loans
- Taking a pension advance
- Dealing with medical debt
- Planning for diminished capacity



# Fraud prevention placemats

---

- FREE bulk orders
- Learn about common financial scams.
- Placemats can be used at group meal sites, or by community or faith-based organizations, financial institutions, Native communities, and other groups in a variety of ways.
- Check out the companion resources with tips and information to reinforce the messages on the placemats.

# Latest placemat – Social Security imposter scams

## Scams involving your Social Security number and benefits are on the rise!



### Here are the facts:

- Government employees will not threaten to take away benefits or ask for money or personal information to protect your Social Security card or benefits.
- Scammers can fake your caller ID. So don't be fooled if the call seems to be from the SSA's real phone number (800) 772-1213 or the SSA Inspector General's Fraud Hotline number.
- If a caller asks for your Social Security number, bank account number or credit card information, hang up.

Report suspected scams to the SSA Inspector General at (800) 269-0271 or [oig.ssa.gov/report](https://oig.ssa.gov/report). Visit [IdentityTheft.gov/SSA](https://IdentityTheft.gov/SSA) for more tips.



Consumer Financial  
Protection Bureau

In collaboration with:



Social Security

# Spot scams from a mile away.

Find these five common scam types:

- fraud
- contractor
- free lunch
- identity theft
- tech support

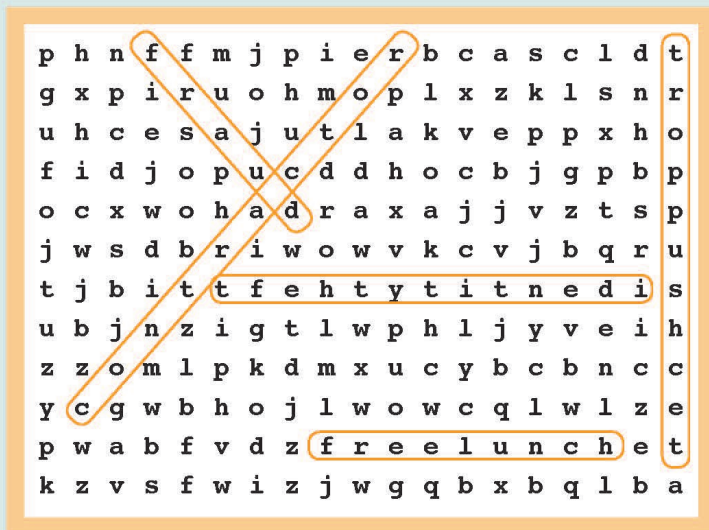


 Answers on back!

p	h	n	f	f	m	j	p	i	e	r	b	c	a	s	c	l	d	t
g	x	p	i	r	u	o	h	m	o	p	l	x	z	k	l	s	n	r
u	h	c	e	s	a	j	u	t	l	a	k	v	e	p	p	x	h	o
f	i	d	j	o	p	u	c	d	d	h	o	c	b	j	g	p	b	p
o	c	x	w	o	h	a	d	r	a	x	a	j	j	v	z	t	s	p
j	w	s	d	b	r	i	w	o	w	v	k	c	v	j	b	q	r	u
t	j	b	i	t	t	f	e	h	t	y	t	i	t	n	e	d	i	s
u	b	j	n	z	i	g	t	l	w	p	h	l	j	y	v	e	i	h
z	z	o	m	l	p	k	d	m	x	u	c	y	b	c	b	n	c	c
y	c	g	w	b	h	o	j	l	w	o	w	c	q	l	w	l	z	e
p	w	a	b	f	v	d	z	f	r	e	e	l	u	n	c	h	e	t
k	z	v	s	f	w	i	z	j	w	g	q	b	x	b	q	l	b	a

# Scams can hide in plain sight, learn how to spot them.

## Answers:



**Fraud:** When someone tricks you into giving up your money.

**Contractor scam:** If someone knocks on your door with an offer to work on your home at a discount, it could be a scam. Often these scam artists charge more than their quoted prices or their work doesn't live up to their promises.

**Free lunch:** You are invited to hear a pitch for an investment in exchange for a free meal. You will likely get pressured to participate. Remember, if it sounds too good to be true, it probably is.

**Identity theft:** When credit cards or bank accounts are opened in your name without your permission. Check bank and credit card statements, and your credit report on a regular basis.

**Tech support scam:** When scammers pretend to be techs who have detected viruses or other malware on your computer. They may try to convince you to buy fake security software, giving them access to your credit card number. Don't give out financial information on an unsolicited call.

# No deje que le roben el corazón, y su billetera.

Una estafa "romántica" es cuando alguien le dice que le ama, pero lo que realmente quiere es su dinero. A veces, puede que ni siquiera sea quien dice ser.



## Preste atención a estas señales de advertencia:

- Su nuevo amor vive lejos y le pide que le envíe dinero o que comparta su número de tarjeta de crédito (aún si le promete que se lo devolverá).
- Su nuevo amor le pide que firme un documento para entregarle el control sobre sus finanzas o su casa.
- Su nuevo amor le pide que abra una nueva cuenta conjunta o que firme un préstamo con él o ella como codeudor.
- Su nuevo amor le pide acceso a sus cuentas bancarias o de tarjetas de crédito.

Denuncie las estafas románticas a la policía, o en línea en [FTC.gov/complaint](https://www.ftc.gov/complaint).

# Don't play games with your credit

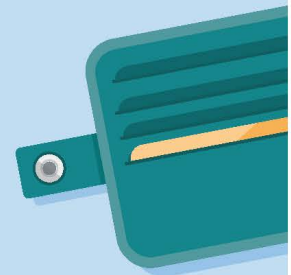
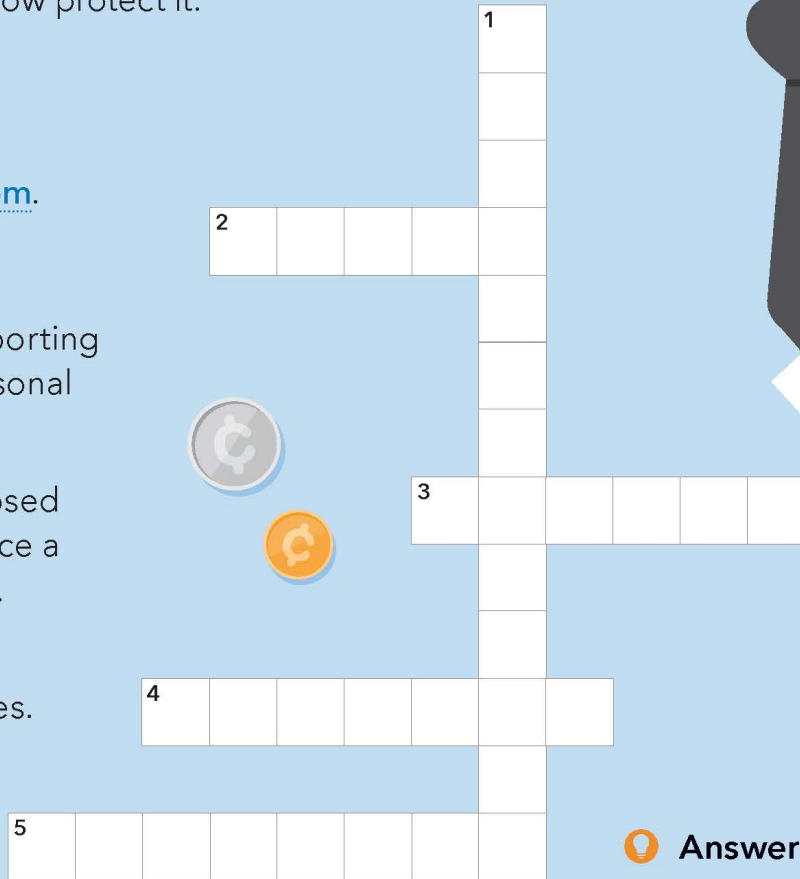
You spend your life building your credit. Now protect it.

## Down

- 1 You can get free \_\_\_\_\_ each year from [annualcreditreport.com](https://annualcreditreport.com).

## Across

- 2 Place a \_\_\_\_\_ alert with the credit reporting companies if someone uses your personal information to open a new account.
- 3 If your personal information was exposed in a data breach, you may want to place a security \_\_\_\_\_ on your credit report.
- 4 Regularly \_\_\_\_\_ your bank and credit card statements for fraud and mistakes.
- 5 \_\_\_\_\_ includes when someone uses your personal information to open new accounts in your name.



 Answers on back!

# Answers



Report identity theft to police and to the FTC at [ftc.gov/complaint](https://www.ftc.gov/complaint) and to each of the three largest credit reporting companies.

## Equifax

Security Freeze: (800) 685-1111

Place a fraud alert: (888) 766-0008

## Experian

Security Freeze: (888) 397-3742

Place a fraud alert: (888) 397-3742

## TransUnion

Security Freeze: (800) 680-7289

Place a fraud alert: (888) 909-8872



# Elder Fraud Prevention and Response Networks

---



The Bureau’s Office of Financial Protection for Older Americans studied the benefits of community networks nationwide that bring together key partners like law enforcement, financial institutions, and adult protective services to protect seniors from financial exploitation.

- The Bureau released a report based on this study, *Fighting Elder Financial Exploitation through Community Networks*.
- The Bureau embarked on an outreach initiative called the Community Protection Networks Project (CPNP) to “seed” the formation of new networks where none exist and help those that are functioning to grow in size or scope and/or enhance their impact.

# Contact Us

---

Consumer Financial Protection Bureau  
Office for Older Americans

Website: [consumerfinance.gov/olderamericans](https://consumerfinance.gov/olderamericans)

Email: [olderamericans@cfpb.gov](mailto:olderamericans@cfpb.gov)

Michael Herndon

[Michael.Herndon@cfpb.gov](mailto:Michael.Herndon@cfpb.gov)

Shanell Blunt

[Shanell.Blunt@cfpb.gov](mailto:Shanell.Blunt@cfpb.gov)



Consumer Financial  
Protection Bureau

# Preventing Elder Financial Exploitation: Trends, Tips & Tools

Lisa Schifferle, Federal Trade Commission

# TRENDS

The background features abstract, overlapping geometric shapes in various shades of blue, ranging from light to dark. These shapes are primarily located on the right side of the page, creating a modern, layered effect. The word 'TRENDS' is centered in a dark blue, sans-serif font.

CONSUMER  
SENTINEL  
NETWORK  
DATA BOOK 2018

SNAPSHOT

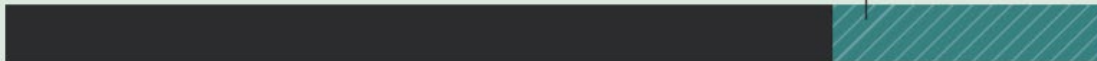
**3**  
**MILLION**  
**REPORTS**

**TOP THREE CATEGORIES**

- 1. Imposter scams**
- 2. Debt collection**
- 3. Identity theft**

**1.4 million** fraud reports

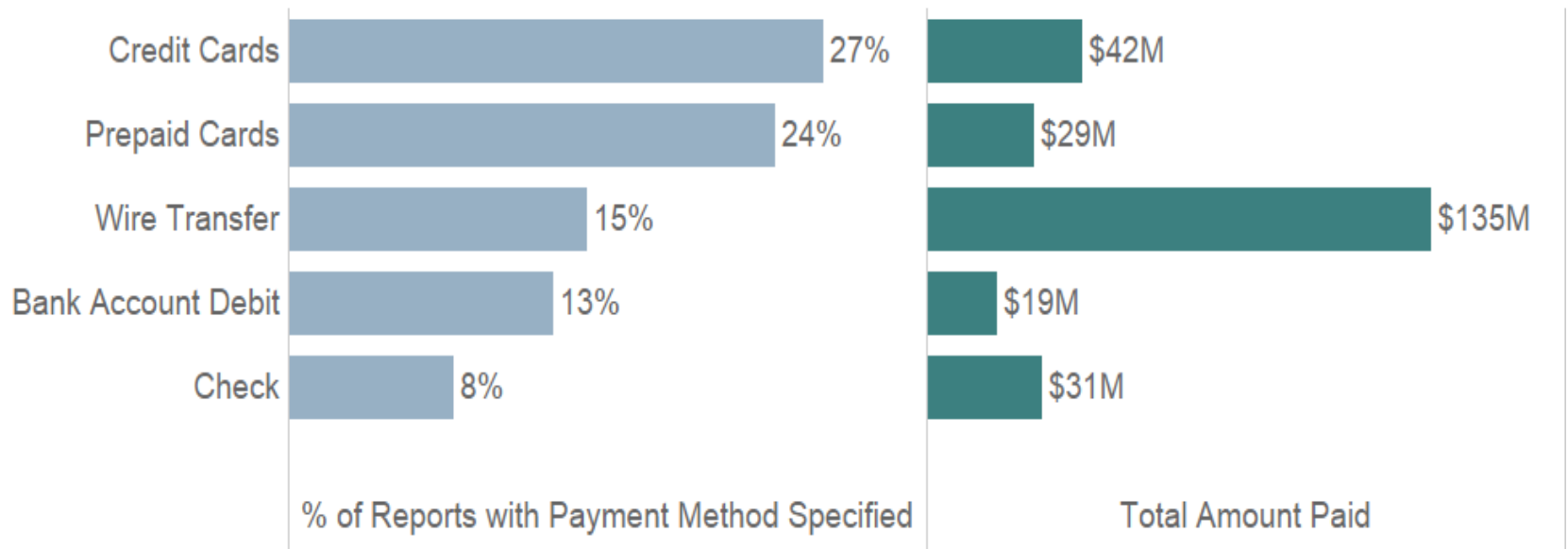
**25%** reported  
a loss



**\$1.48 billion**  
total fraud losses

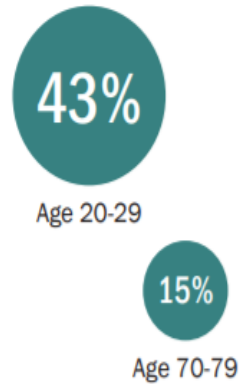
**\$375**  
median loss

## TOP PAYMENT METHODS AND TOTAL AMOUNT PAID (AGES 60 AND OVER) 2018

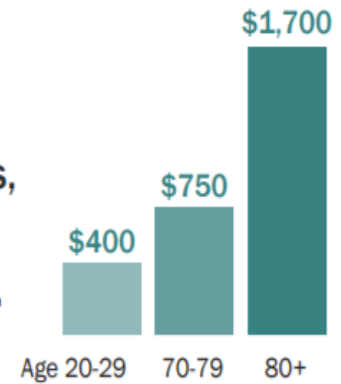


# Fraud & Age

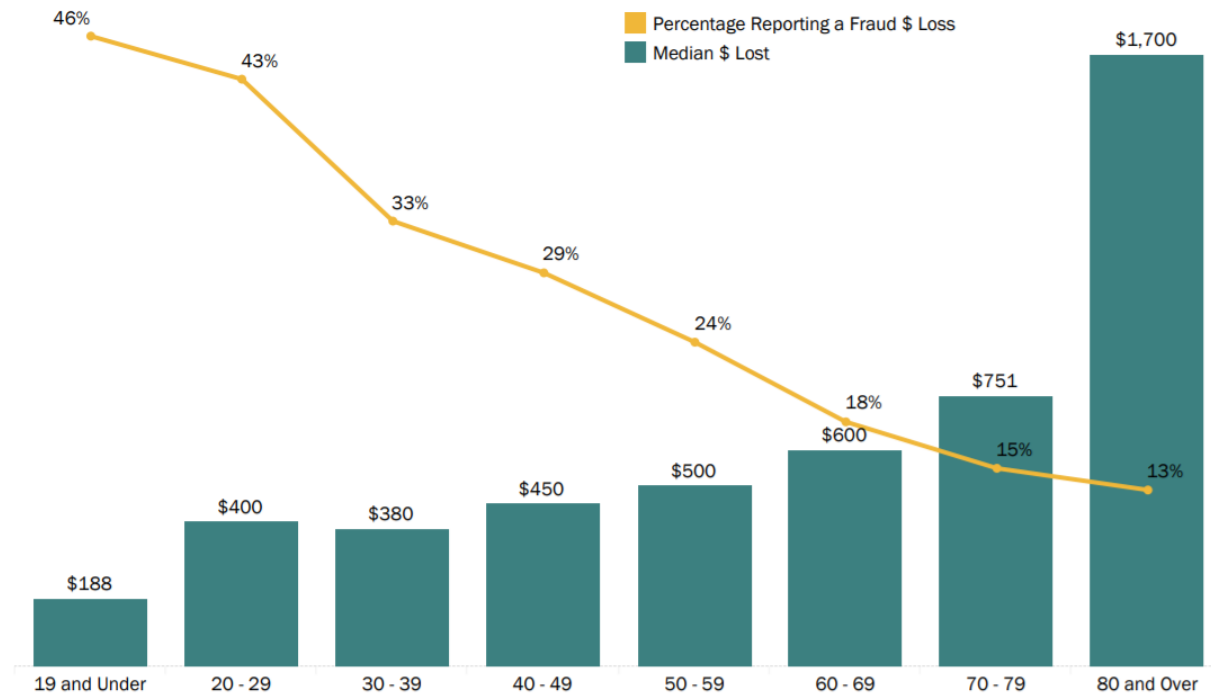
**Younger people reported losing money to fraud more often than older people.**



**But when people aged 70+ had a loss, the median loss was much higher.**



### Percentage Reporting a Fraud Loss and Median Loss by Age



Of the 1,427,563 total fraud reports in 2018, 46% included consumer age information.



**TIPS**

The background features abstract, overlapping geometric shapes in various shades of blue, ranging from light to dark. These shapes are primarily located on the right side of the page, creating a modern, layered effect. The rest of the page is a plain white background.



# Types of Scams

- Imposter Scams
- Charity Scams
- Health Care Scams
- You've Won Scams



# Imposter Scams





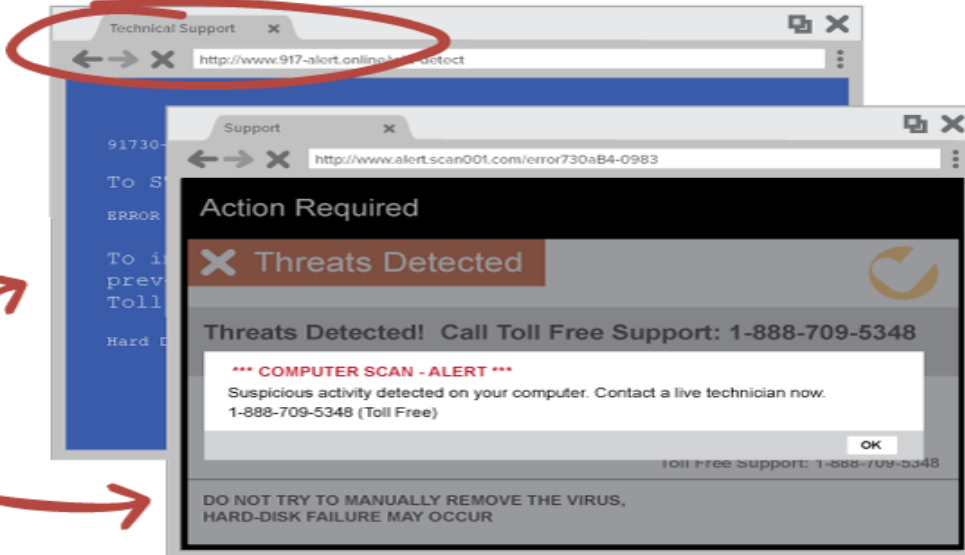
## Tech Support Scams – How they work

- Older adults 5x more likely to report this scam
- Call pretending to be from or affiliated with computer security companies, such as Dell, Microsoft, Norton, or others.
- Scare consumers about their computer security
- Often want to remotely access the consumer's computer and sell software or services.

# HOW TO SPOT A TECH SUPPORT SCAM

It often starts with a pop-up . . .

Shows up within your internet browser



Might imitate a blue error screen or trusted antivirus software

## CALL

Wants you to call a toll-free number

## NOW

Urges you to call immediately

## OR ELSE...

Threatens that you may lose personal data if you don't call



# Tech Support Scams - Tips

## → HANG UP.

- Never give control of your computer or your credit card information to someone who calls you out of the blue.

## → PASS IT ON.



# Tech Support Scams Video



# Online Dating Scams







# Online Dating Scams – How they work

- You meet someone on a dating website.
- She wants to communicate by email and phone.
- She says she loves you but needs money for a plane ticket to visit. Or for surgery.
- She asks you to wire money or put it on a prepaid card.



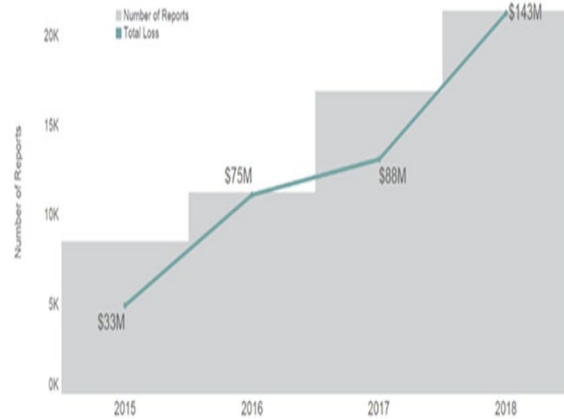
## Online dating scams - Tips

- STOP. Don't send money.
  - Never wire money, put money on a prepaid card or send cash to an online love interest.
  - You won't get it back.
- PASS IT ON.

# Romance Scams

## Romance Scam Reports Over Time

Reports more than doubled and reported losses increased more than fourfold from 2015 to 2018



# \$2,600

The **median reported loss** to romance scams is about seven times higher than for other frauds (2018).



# Grandkid Scams





# Grandkid Scams



- You get a call: “grandma, I need money for bail.”
  - Or a medical bill
  - Or other trouble
- Caller says it’s urgent and says to keep it a secret
- Caller asks you to wire money or put it on a prepaid card



# Grandkid Scams – Tips

- ➔ STOP. Check it out.
  - Look up your grandkid's phone number and call back
  - Or call another family member
- ➔ PASS IT ON.



# Family Emergency Scam Video



# IRS Imposter Scams







# IRS Imposter Scams – How they work

Scammers may:

- Rig caller ID to make it look like call is from Washington DC (202 area code)
- Demand immediate payment by pre-paid debit card or wire transfer
- Send bogus IRS emails to further the scheme



# New IRS Imposters Video



# IRS Imposter Scams - Tips

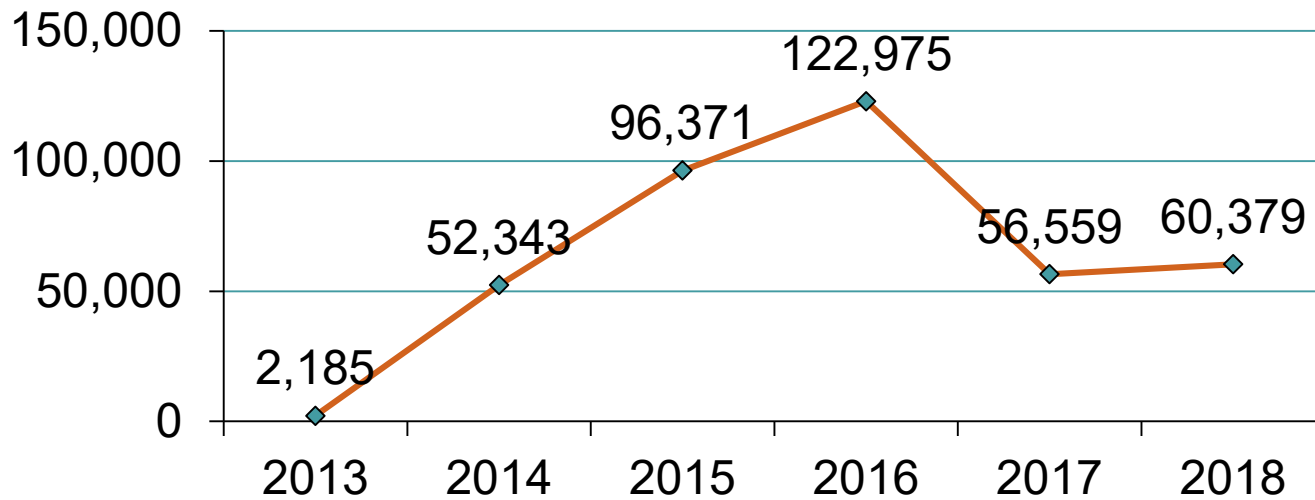
The IRS will NOT:

- ask you to pay with prepaid debit cards or wire transfers
- ask for a credit card over the phone
- threaten arrest, deportation or loss of your drivers license
- Initiate contact by email

→ STOP. Don't wire money or pay with a prepaid debit card.

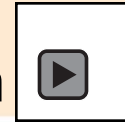


# IRS Imposter Scams





## Social Security Administration



## Imposters

- Claim your SSN has been suspended because of suspicious activity, or it's been involved in a crime.
- Ask you to confirm your SSN, or say you need to withdraw money from the bank and store it on gift cards for "safekeeping."
- May say your accounts will be seized or frozen if you don't act quickly.



## SSA Imposter Tips

- Your SSN is not about to be suspended!
- The real SSA will not call out of the blue or tell you to wire money, send cash, or put money on gift cards.
- Don't trust caller ID.
- Don't give the caller your Social Security number or other personal information.
- Visit [IdentityTheft.gov/SSA](https://www.identitytheft.gov/SSA) to learn more.



# Charity Scams





# Charity Fraud – How it Works

→ Here's how it works:

- Phone call
- Charity name sounds familiar
- Pressure you to pay quickly





# Charity Fraud – What You Can Do

- ➔ Take your time
- ➔ Say no
  - “No, thanks.” Hang up. ...OR:
  - “I don’t give money over the phone. If you send something in writing, I’ll consider it.”
- ➔ Never send cash, wire money or load prepaid debit cards



# Health Care Scams





# Health Care Scams – How It Works

- They'll say you need...
  - A new Medicare card
  - A new health insurance card
  - Discounted health insurance
  - To act now!



# New Medicare Cards April 2018 - March 2019

**New Card! New Number!**

*Mailing in 2018*

**Current Medicare Card**

**MEDICARE HEALTH INSURANCE**

1-800-MEDICARE (1-800-633-4225)

NAME OF BENEFICIARY  
**JANE DOE**

MEDICARE CLAIM NUMBER  
**000-00-0000-A**

SEX  
**FEMALE**

IS ENTITLED TO  
**HOSPITAL (PART A) 07-01-2016**  
**MEDICAL (PART B) 07-01-2016**

SIGN HERE → *Jane Doe*

**NEW Medicare Card**


**MEDICARE HEALTH INSURANCE**

Name/Nombre  
**JOHN L SMITH**

Medicare Number/Número de Medicare  
**1EG4-TE5-MK72**

Entitled to/Con derecho a  
**HOSPITAL (PART A) 03-01-2016**  
**MEDICAL (PART B) 03-01-2016**

Coverage starts/Cobertura empieza



CMS Product No. 12000-P  
September 2017



# Health Care Scams – What You Can Do

- Take your time
- Check it out
  - 1-800-MEDICARE
- Consult reliable sources of health information (healthcare.gov, cdc.gov)
- Do not delay medical treatment



# “You’ve Won” Scams





## **“You’ve Won” Scams— How They Work**

- You get a call, an email, a card
- Says that you’ve won a prize, lottery, trip
- You just need to pay fees, taxes, custom fees first
- They want you to wire money or give your credit card information



## “You’ve Won” Scams – What You Can Do

- What you can do:
- Keep your money to yourself
  - Keep your information to yourself
  - If in doubt, check it out
  - Never wire money



**TOOLS**

The background features abstract, overlapping geometric shapes in various shades of blue, ranging from light to dark. These shapes are primarily located on the right side of the frame, creating a modern, layered effect against the white background.



- Consumer education for active older adults – [www.ftc.gov/passiton](http://www.ftc.gov/passiton)
- Respecting a lifetime of experience
- Encouraging sharing of information on:



identity theft



health care scams



imposter scams



paying too much



charity fraud



“you’ve won” scams



# Sample Article



## Health Care Scams

### Here's how they work:


You see an ad on TV, telling you about a new law that requires you to get a new health care card. Maybe you get a call offering you big discounts on health insurance. Or maybe someone says they're from the government, and she needs your Medicare number to issue you a new card.

Scammers follow the headlines. When it's Medicare open season, or when health care is in the news, they go to work with a new script. Their goal? To get your Social Security number, financial information, or insurance number.

So take a minute to think before you talk: Do you really have to get a new health care card? Is that discounted insurance a good deal? Is that



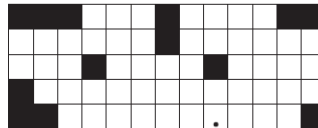
# Sample Activity



## Identity Theft Activity

Solve the fallen phrase.

All the letters in this phrase have fallen to the bottom. They were mixed up on their way down, but remain in the same column.



ER T FR  
ENUO Y PDI  
ARGITECOEOT  
FOREPARRURMT  
CRNDF TLEECORM





FEDERAL TRADE COMMISSION

IdentityTheft.gov

Log In

En Español

Report identity theft and get a recovery plan

Get Started →

or browse recovery steps

IdentityTheft.gov can help you report and recover from identity theft.

**HERE'S HOW IT WORKS:**



**Tell us what happened.**

We'll ask some questions about your situation. Tell us as much as you can.



**Get a recovery plan.**

We'll use that info to create a personal recovery plan.



**Put your plan into action.**

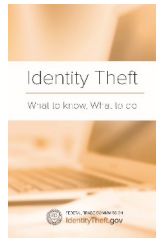
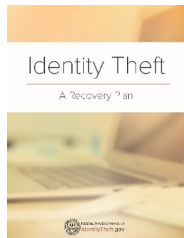
If you create an account, we'll walk you through each recovery step, update your plan as needed, track your progress, and pre-fill forms and letters for you.

[Get started now.](#) Or you can [browse a complete list of possible recovery steps](#).

# Identity Theft

Free print materials to order:

[www.ftc.gov/bulkorder](http://www.ftc.gov/bulkorder)







# Unwanted Calls

[ftc.gov/calls](https://ftc.gov/calls)


## How to stop unwanted calls ON A LANDLINE



See what services your **carrier** offers.




Some services are **free**, but others charge a monthly **fee**.



Install a **call-blocking device**.  
Some use **blacklists** to

- stop unwanted calls
- divert calls to voicemail

Some use **whitelists** of approved numbers.



Report unwanted calls at [ftc.gov/complaint](https://ftc.gov/complaint)

FEDERAL TRADE COMMISSION • [ftc.gov/calls](https://ftc.gov/calls)



# Hypotheticals







## Hypo – Tech Support Scam

- Janet was using her computer when screen locked and a message appeared saying that all of his credit card and social media information would be taken off the computer immediately unless she called tech support at 1-800-GET-HELP.
- she called the number, let them remote into the computer and gave his credit card information to try to get her computer fixed. She thought everything was great until she talked to her daughter who thought it was a scam.



## Hypo – Online Dating Scam

- Sally lost her husband about two years ago. Friends have encouraged her to try dating again. She's in a rural community so she decides to try online dating to have a bigger pool of older men to choose from.
- She meets someone online and emails with him for weeks. He says he loves her and wants to come meet her but needs money for surgery first. She wires \$10k and he tells her how she saved his life and he loves her more than ever. Now, he wants money for a plane ticket to come see her. She wires another \$1,000 but he never arrives.