

# Cybercriminals are after us

**GVR Computer Club**

**April 5, 2022**

# Brought to you by....

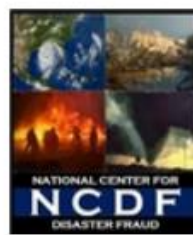
- APCUG's Speakers Bureau, a benefit of your group's membership in APCUG
  - Judy Taylour, President, SCV Computer Club
  - APCUG Advisor – Regions 10, 11, and International
    - jtaylour (at) apcug.org



# Consumer Sentinel Network Data Book 2021

## 2021 Fraud Results

**Federal Trade Commission**  
February 2022



# 2021 Fraud Results

## Imposter Scams



ABOUT  
**1 in 5**  
**PEOPLE**  
LOST MONEY

\$2,331 million  
reported lost  
\$1,000 median loss

## Identity Theft Reports

64% 

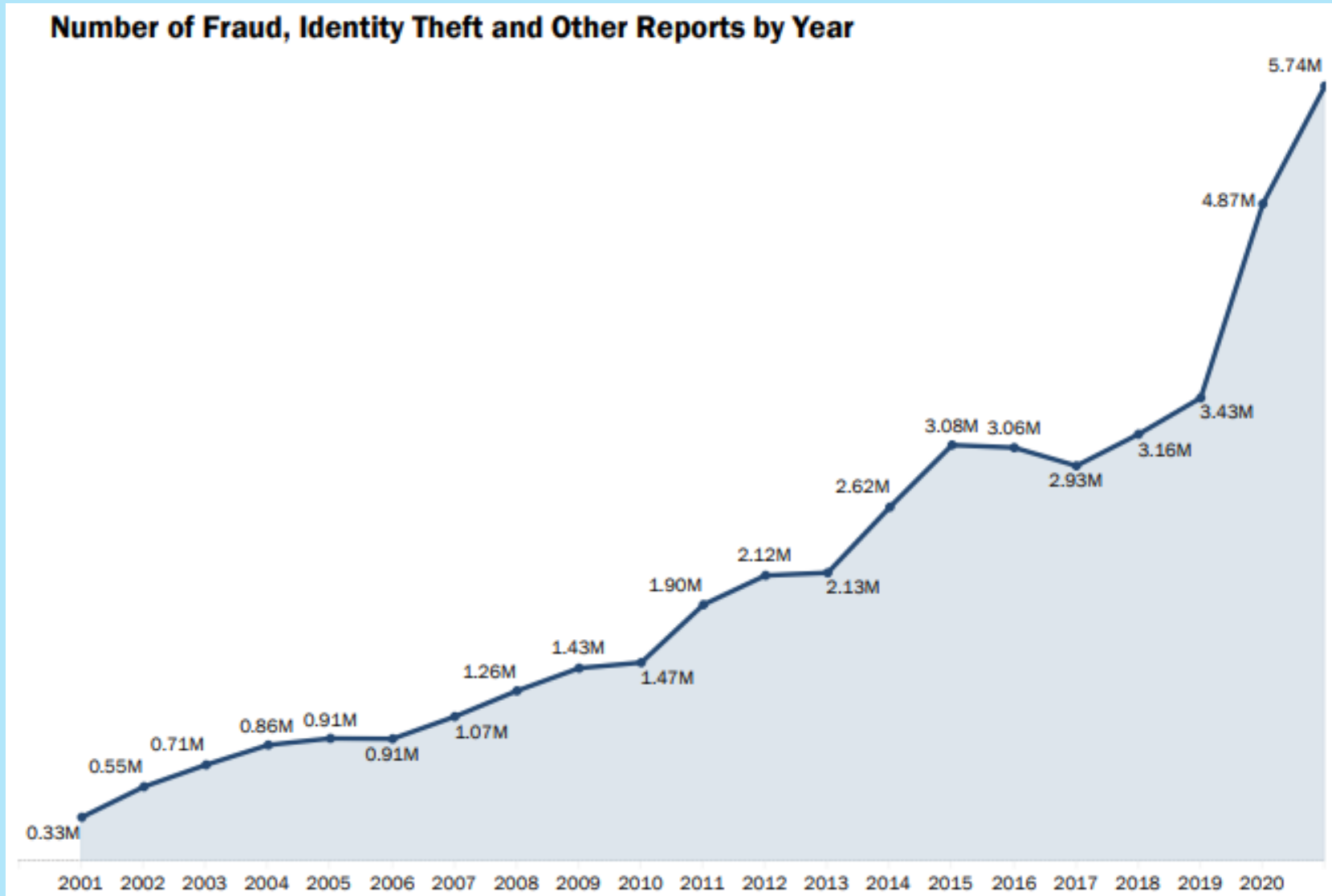
Checking\Savings  
Account - New

22% 

Mobile  
Telephone –  
New Accounts

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

# 2021 Fraud Results



# 2021 Fraud Results

## Report Categories

Rank	Category	# of Reports	%
1	Identity Theft	1,434,676	25.01%
2	Imposter Scams	984,756	17.16%
3	Credit Bureaus, Information Furnishers and Report Users	592,928	10.33%
4	Online Shopping and Negative Reviews	398,283	6.94%
5	Banks and Lenders	195,370	3.41%
6	Debt Collection	151,335	2.64%
7	Prizes, Sweepstakes and Lotteries	148,243	2.58%
8	Auto Related	137,468	2.40%
9	Internet Services	121,445	2.12%
10	Business and Job Opportunities	104,019	1.81%
11	Telephone and Mobile Services	92,802	1.62%
12	Health Care	89,801	1.57%
13	Investment Related	78,988	1.38%
14	Home Repair, Improvement and Products	70,612	1.23%
15	Privacy, Data Security, and Cyber Threats	70,177	1.22%

16	Credit Cards	65,173	1.14%
17	Travel, Vacations and Timeshare Plans	53,891	0.94%
18	Television and Electronic Media	41,905	0.73%
19	Foreign Money Offers and Fake Check Scams	39,139	0.68%
20	Advance Payments for Credit Services	24,152	0.42%
21	Education	22,810	0.40%
22	Mortgage Foreclosure Relief and Debt Management	21,258	0.37%
23	Computer Equipment and Software	15,701	0.27%
24	Charitable Solicitations	9,270	0.16%
25	Magazines and Books	5,541	0.10%
26	Tax Preparers	5,424	0.09%
27	Grants	4,254	0.07%
28	Office Supplies and Services	3,609	0.06%
29	Funeral Services	1,310	0.02%

# 2021 Fraud Results

## Top 10 Fraud Categories

Rank	Category	# of Reports	% Reporting \$ Loss	Total \$ Loss	Median \$ Loss
1	Imposter Scams	984,756	17%	\$2,331M	\$1,000
2	Online Shopping and Negative Reviews	397,826	52%	\$392M	\$150
3	Prizes, Sweepstakes and Lotteries	148,243	12%	\$255M	\$968
4	Internet Services	103,501	23%	\$216M	\$500
5	Business and Job Opportunities	103,003	25%	\$206M	\$1,991
6	Telephone and Mobile Services	92,716	12%	\$21M	\$250
7	Investment Related	78,988	73%	\$1,679M	\$3,000
8	Health Care	63,333	13%	\$17M	\$197
9	Travel, Vacations and Timeshare Plans	53,891	24%	\$95M	\$1,112
10	Foreign Money Offers and Fake Check Scams	39,139	26%	\$78M	\$2,000



# 2021 Fraud Results

## Identity Theft Types

Rank	Theft Type	# of Reports
1	Government Documents or Benefits Fraud	395,948
2	Credit Card Fraud	389,737
3	Other Identity Theft	377,102
4	Loan or Lease Fraud	197,914
5	Bank Fraud	124,388
6	Employment or Tax-Related Fraud	111,723
7	Phone or Utilities Fraud	88,813

## Top 10 Other Categories

Rank	Category	# of Reports
1	Credit Bureaus, Information Furnishers and Report Users	592,928
2	Banks and Lenders	195,370
3	Debt Collection	151,335
4	Auto Related	137,468
5	Home Repair, Improvement and Products	70,612
6	Credit Cards	65,173
7	Television and Electronic Media	41,905
8	Education	22,810
9	Privacy, Data Security, and Cyber Threats	18,724
10	Computer Equipment and Software	15,701



# 2021 Fraud Results

## Fraud Reports by Amount Lost

2,789,161

Number of Fraud Reports

692,376 (25%)

# of Reports with \$ Loss

\$5,893,260,382

Total \$ Loss

\$500

Median \$ Loss

## Reported Fraud Losses in \$1 - \$10,000+ Range

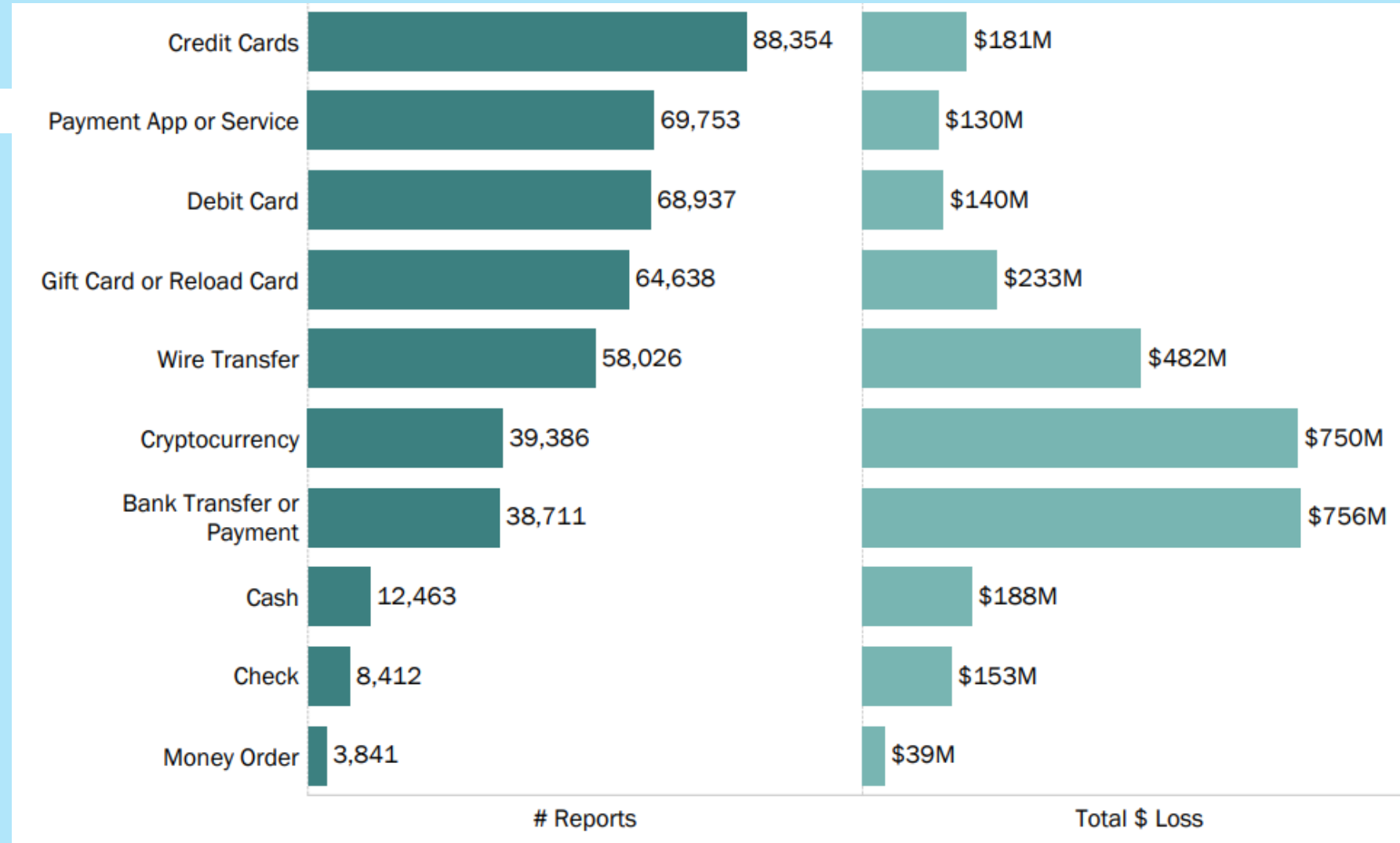
Amount Lost	# of Reports
\$1 - \$1,000	447,732
\$1,001 - \$2,000	74,179
\$2,001 - \$3,000	35,101
\$3,001 - \$4,000	19,743
\$4,001 - \$5,000	16,112
\$5,001 - \$6,000	9,425
\$6,001 - \$7,000	6,804
\$7,001 - \$8,000	6,034
\$8,001 - \$9,000	4,215
\$9,001 - \$10,000	7,496
More than \$10,000	65,535

## Reported Fraud Losses in \$1 - \$1,000 Range

Amount Lost	# of Reports
\$1 - \$100	168,469
\$101 - \$200	74,439
\$201 - \$300	45,080
\$301 - \$400	32,212
\$401 - \$500	35,141
\$501 - \$600	21,421
\$601 - \$700	15,971
\$701 - \$800	18,159
\$801 - \$900	12,044
\$901 - \$1,000	24,796

# 2021 Fraud Results

## Fraud Reports by Payment Method

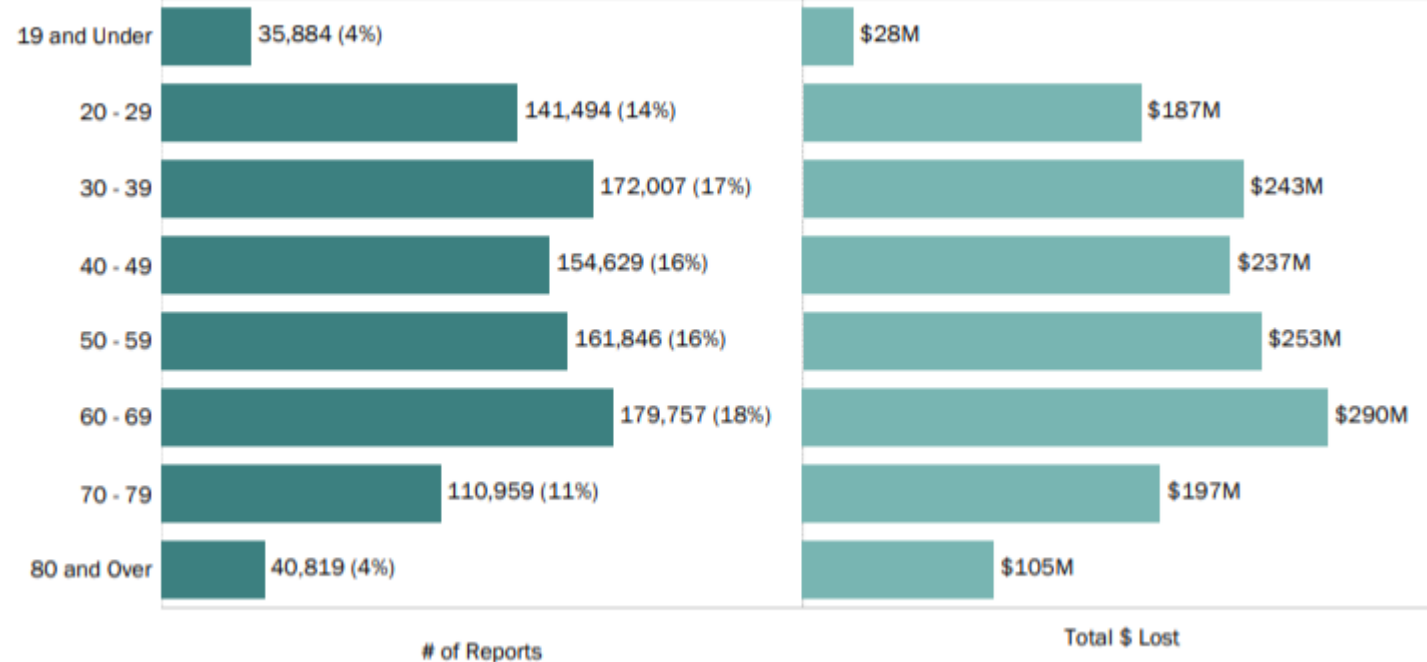


# 2021 Fraud Results

## Number of Reports and Amount Lost by Contact Method

Contact Method	# of Reports	Total \$ Lost	Median \$ Lost
Phone call	383,598	\$436M	\$1,170
Text	334,524	\$86M	\$800
Email	186,621	\$247M	\$400
Website or Apps	134,416	\$316M	\$150
Other	100,926	\$314M	\$234
Social Media	70,365	\$257M	\$200
Mail	35,878	\$46M	\$799
Online Ad or Pop-up	6,884	\$13M	\$172

## Reported Frauds and Losses by Age



Percentages are based on the total number of 2020 fraud reports in which consumers provided their age: 997,395.

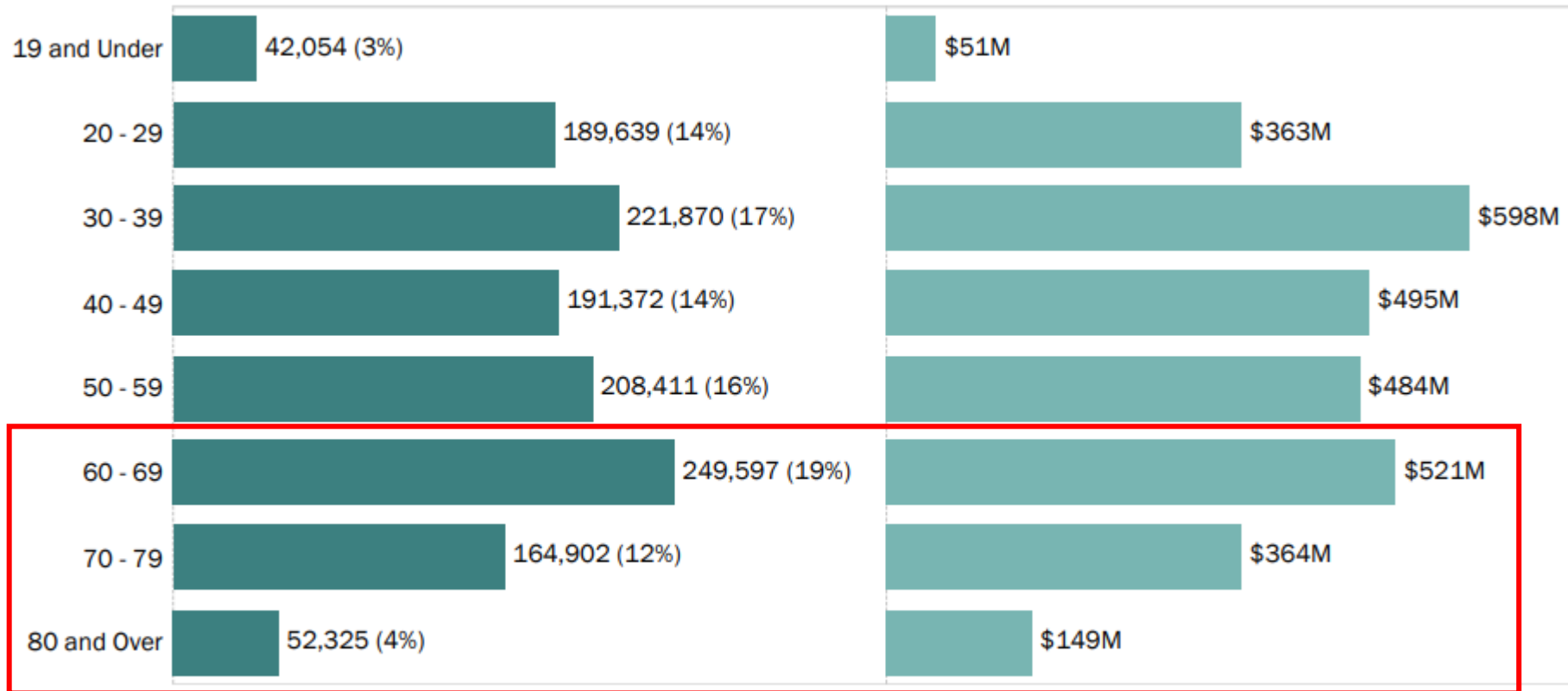
# 2021 Fraud Results

## Number of Reports and Amount Lost by Contact Method

Contact Method	# of Reports	Total \$ Lost	Median \$ Lost
Phone call	644,048	\$692M	\$1,200
Text	377,840	\$131M	\$900
Email	260,818	\$323M	\$800
Website or Apps	177,777	\$649M	\$300
Social Media	159,423	\$796M	\$400
Other	114,354	\$677M	\$622
Mail	42,842	\$65M	\$823
Online Ad or Pop-up	36,730	\$96M	\$181

# 2021 Fraud Results

## Reported Frauds and Losses by Age



# of Reports

Total \$ Lost

Percentages are based on the total number of 2021 fraud reports in which consumers provided their age: 1,320,170.

# 2021 Fraud Results - Arizona

## State Rankings: Fraud and Other Reports

Rank	State	Reports per 100K Population	# of Reports
15	New York	1,083	210,749
16	Texas	1,080	313,044
17	Illinois	1,078	136,640
18	Rhode Island	1,066	11,289
19	Arizona	1,065	77,534
20	North Carolina	1,036	108,698
21	Washington	1,013	77,128
22	California	991	391,517
23	Massachusetts	980	67,515
24	Ohio	976	114,140

## State Rankings: Identity Theft Reports

Rank	State	Reports per 100K Population	# of Reports
10	Florida	515	110,675
11	Texas	504	146,095
12	Maryland	493	29,778
13	Ohio	431	50,421
14	Pennsylvania	425	54,460
15	Alabama	402	19,691
16	Arizona	386	28,108
17	New Jersey	359	31,857
18	South Carolina	343	17,642
19	California	337	133,119

# 2021 Fraud Results - Arizona

## Fraud & Other Reports

19th

State Rank  
(Reports per 100K Population)

77,534

Total Fraud & Other Reports

## Fraud Losses

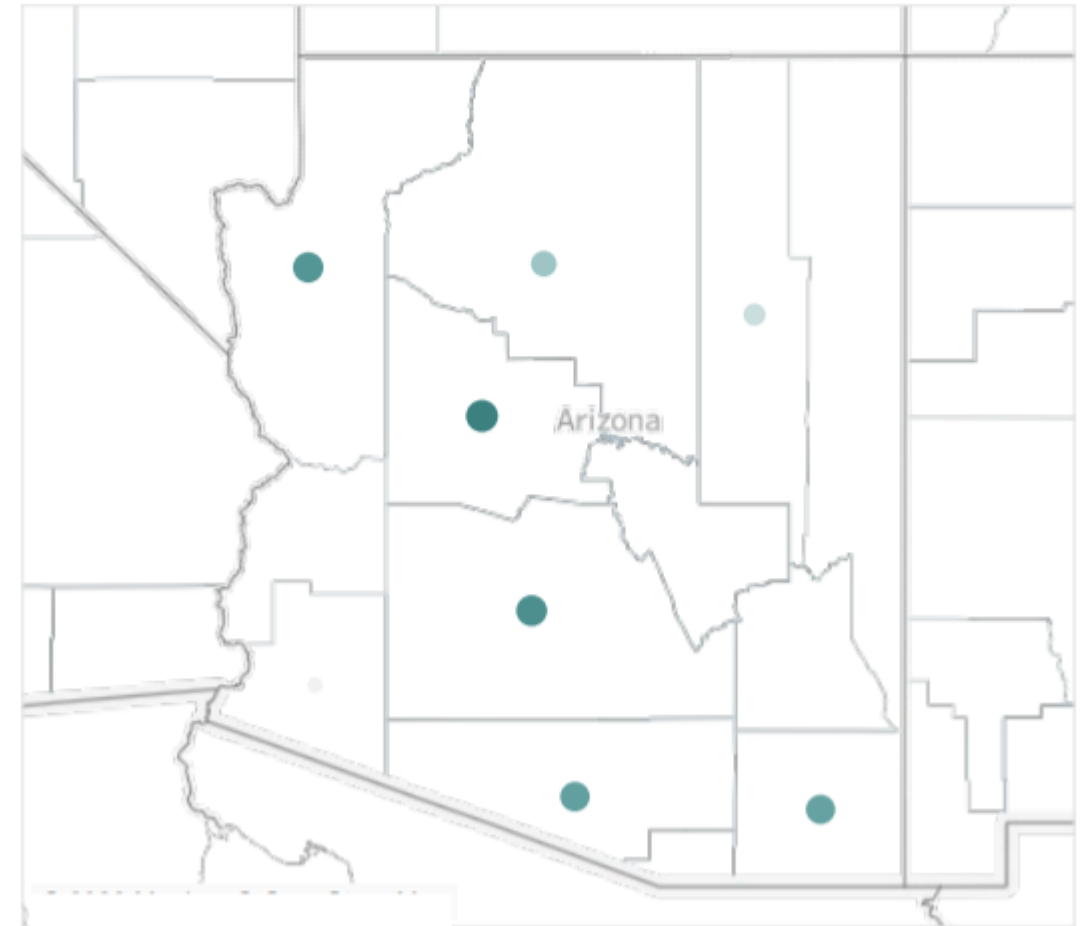
\$116.0M

Total Fraud Losses

\$515

Median Fraud Losses

## Fraud & Other Reports by Metropolitan Area



## Identity Theft Reports

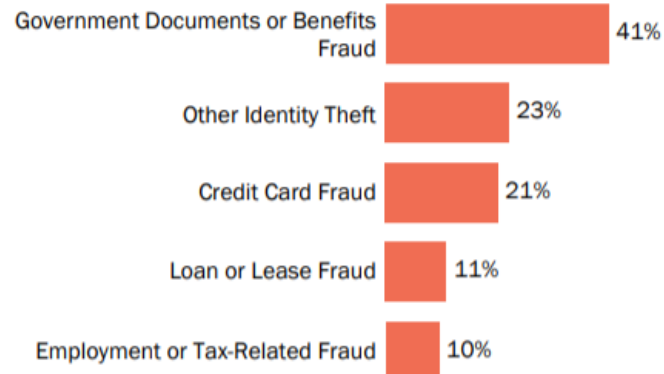
Reports per 100K Population

572

●

1,186

## Top Identity Theft Types



## Identity Theft Reports

16th

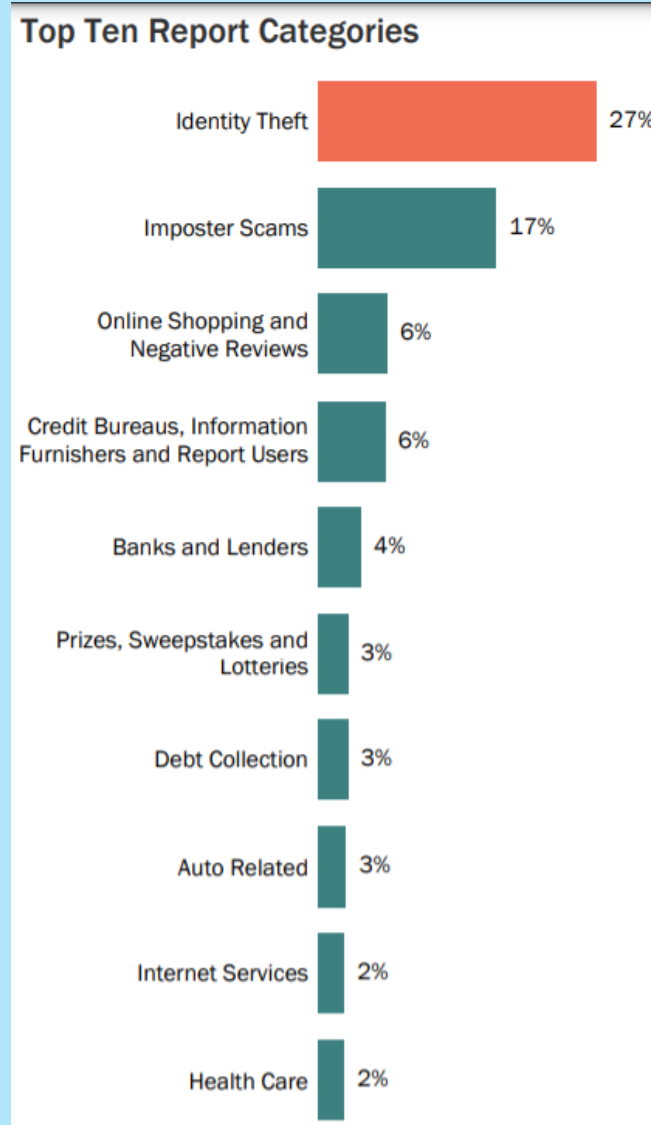
State Rank  
(Reports per 100K Population)

28,108

Identity Theft Reports



# 2021 Fraud Results - Arizona



# From the FBI

## Common Elder Fraud Schemes – a long list

- Advance Fee
- Charity and Disaster Fraud
- Counterfeit Prescription Drugs
- Credit Card Fraud
- Election Crimes and Security
- Cosmetic and “Anti-Aging” Products
- Fundal and Cemetery Fraud

More Information

[Common Scams and Crimes — FBI](#)



# From the FBI

## **Common Elder Fraud Schemes – a long list**

- Healthcare Fraud
- Holiday Scams
- ID Theft
- Internet Auction Fraud
- Investment Fraud
- Market Manipulation (Pump and Dump) Fraud
- Money Mules
- Nigerian Letter or “419” Fraud

# From the FBI

## **Common Elder Fraud Schemes – a long list**

- Non-Delivery of Merchandise
- Online Vehicle Sale Fraud
- Ponzi Schemes
- Prime Bank Note Fraud
- Pyramid Schemes
- Ransomware
- Redemption/Strawman/Bond Fraud
- Reverse Mortgage Scams
- Romance Scams

# From the FBI

- **Government impersonation scam:** Criminals pose as government employees and threaten to arrest or prosecute victims unless they agree to provide funds or other payments.
- **Home repair scam:** Criminals appear in person and charge homeowners in advance for home improvement services that they never provide.
- **TV/radio scam:** Criminals target potential victims using illegitimate advertisements about legitimate services, such as reverse mortgages or credit repair.
- **Family/caregiver scam:** Relatives or acquaintances of the elderly victims take advantage of them or otherwise get their money.

# From the FBI

## Protect Yourself

- **Never give or send any personally identifiable information**, money, jewelry, gift cards, checks, or wire information to unverified people or businesses.
- **Make sure all computer anti-virus and security software and malware protections are up to date.** Use reputable anti-virus software and firewalls.
- **Disconnect from the internet and shut down your device if you see a pop-up message or locked screen.** Pop-ups are regularly used by perpetrators to spread malicious software. Enable pop-up blockers to avoid accidentally clicking on a pop-up.

# From the FBI

## Protect Yourself

- **Be careful what you download.** Never open an email attachment from someone you don't know and be wary of email attachments forwarded to you.
- **Take precautions to protect your identity** if a criminal gains access to your device or account.
- Immediately contact your financial institutions to place protections on your accounts and monitor your accounts and personal information for suspicious activity.



# Reverse Mortgage Scams

- Often a group effort of bad actors
  - Mortgage brokers
  - Financial advisors
  - Appraisers
  - Attorneys
  - Loan officers
- Inflated appraisal = more money for you

More Information

[Protect Your Home's Equity From Reverse Mortgage Scams \(aarp.org\)](https://aarp.org)



# Reverse Mortgage Scams

- FHA does insure some reverse mortgages
  - Does not protect borrower
  - Does protect lender in case of default
- Get reliable information from HUD or FTC
- Make sure reverse mortgage is a federally insured Home Equity Conversion Mortgage
- You are required by law to meet with a government-approved counselor

# Romance Scams

- People aren't always as they appear
- Each year, tens of thousands of Internet users fall victim to online romance scams – don't be one of them
- Incredibly convincing, increasingly found on dating sites and social media
- Appeal to victim's emotions and feigning personal connections  
scammers try to steal personal information and large sums of money

More Information

[What You Need To Know About Romance Scams | Consumer Information \(ftc.gov\)](#)



# Romance Scams

## Look out for red flags

- Request for money
- Claims to live overseas or is in the military
- Professes love quickly
- Pressure to move conversation to another platform/different site

# Romance Scams

## Take Action

- Cease communications immediately
- Notify website or app where you met the scammer
- What identifiable information do you have on the scammer
  - Email address
  - IP address
  - Any other information
- Have you sent money?
  - Contact bank or credit card company
- Report scammer to FTC – [ftc.gov/complaint](https://ftc.gov/complaint)

# Ransomware 101

- Type of malicious software that infects a computer and restricts users' access to it until a ransom is paid to unlock it.

## How do you get it?

- Phishing emails that look legitimate but contain malicious code.
- Drive-by downloading by unknowingly visiting an infected website and then malware is downloaded and installed without your knowledge.
- Social media
- Web-based instant messaging applications

More Information

[What to Do If a Ransomware Attacks Your Computer \(aarp.org\)](https://aarp.org/what-to-do-if-a-ransomware-attacks-your-computer)



# Ransomware 101

## How do you get it?

- You get a pop-up
  - “Your computer has been infected with a virus. Click here to resolve the issue.”
  - If you ‘click here’ it really downloads to your hard drive
  - “Your computer was used to visit websites with illegal content. To unlock your computer, you must pay a \$100 fine.”
  - “All files on your computer have been encrypted. You must pay this ransom within 72 hours to regain access to your data.”
- Don’t click on ‘X’ in the upper right corner
- Alt+F4 should close the pop-up or shut down your computer



# Ransomware 101

## How do you get it?

- You get a pop-up
  - “Your computer has been infected with a virus. Click here to resolve the issue.”
  - If you ‘click here’ it really downloads to your hard drive
  - “Your computer was used to visit websites with illegal content. To unlock your computer, you must pay a \$100 fine.”
  - “All files on your computer have been encrypted. You must pay this ransom within 72 hours to regain access to your data.”
- Don’t click on ‘X’ in the upper right corner

# Ransomware 101

## What should you do?

- Use Alt+F4 to close the open window or pop-up
- Shut down your computer and see if you can access your files
  - Run Malwarebytes
  - Do a deep scan with your anti-virus program

# Ransomware 101

## **If your files are locked – should you pay?**

- Paying the ransom does not guarantee the encrypted files will be released; it only guarantees that the malicious actors receive the victim's money, and in some cases, their banking information.
- In addition, decrypting files does not mean the malware infection itself has been removed.
- Report what happened to your local police
- Report the incident to the FBI's Internet Crimes Complaint Center

# Ransomware 101

## Preventive maintenance

- Only plug in your external drive when you are backing up
- Ransomware can also infect it
- Have a redundant online backup
- Refresh your operating system
  - You will need to reinstall all the apps you downloaded
- Use a Virtual Box when you are out and about on the web
- Be aware of where you click

# Elder Bank Fraud - Money Mule

What is a money mule?

- Someone who transfers or moves illegally acquired money on behalf of someone else
- Money mules add layers of distance between crime victims and criminals, which makes it harder for law enforcement to accurately trace money trails
- Move money through bank accounts, cashier's checks, virtual currency, prepaid debit cards, or money service businesses

More Information

[What's a money mule scam? | Consumer Information \(ftc.gov\)](#)

# Elder Bank Fraud - Money Mule

- Who is targeted?
  - Seniors
  - Students
  - Looking for work
  - Dating sites – romance scams
- If you think you might be involved in a money mule or money transfer scam, stop transferring money
- Notify your bank, the wire transfer service, or any gift card companies involved
- Report it to the FTC at [ftc.gov/complaint](https://www.ftc.gov/complaint).

# Elder Bank Fraud - Money Mule

- Can go to jail even if you don't know what is happening
- Nationwide Money Mule Initiative
  - U.S. Attorney's Office
  - FBI
  - U.S. Secret Service
  - U.S. Postal Inspection Service
- Federal charges you could face include
  - mail fraud
  - wire fraud
  - bank fraud
  - money laundering



# Elder Bank Fraud - Money Mule

## Section 314(b) USA Patriot Act

- Permits financial institutions, upon providing notice to the United States Department of the Treasury, to share information with one another in order to identify and report to the federal government activities that may involve money laundering or terrorist activity.
- Financial Institution Notification 314B Form = takes a long time to get feedback, etc.

## More Information

[What's a money mule scam? | Consumer Information \(ftc.gov\)](#)



# Elder Bank Fraud - Money Mule

## Verifin

- Fraud network exchange
- Banks can join and interface via SMS text messages
- Will get an immediate answer
- Over 3000 banks easily share information
- [314b-collaborate-with-confidence-EB-Verafin-161123.pdf](#)

# Shop Safely Online

## Do your homework

- Think before you click – is the offer too enticing?
- Go to the website to verify if the offer is legitimate
- Prior to making a purchase, read Better Business Bureau reviews to learn what others say about the website/merchant.
- Look for a physical location/phone number (check it out)

# Shop Safely Online

## Do your homework

- Use a credit card – never your debit card
- Use a 3<sup>rd</sup> party payment service – safer than a credit card
  - PayPal, Google Pay, Apple Pay.....
- Do they really need all the information they are asking for?
- Check your bank and credit card statements

# Shop Safely Online

## Privacy

- Privacy gives you control over who can charge you and how much.
- Create virtual payment cards for one-time purchases or subscriptions, directly from your browser.
- Set spending limits, pause, unpause, and close cards any time you want.

More Information

[Privacy - Smarter Payments](#)

Nickname  
No Nickname

Monthly Limit  
No Limit

**Personal**

\$0

Forever



**Everything you need...**

Create up to 12 cards per month

Secure merchant-locked & single-use cards

Set spend limits, pause and close cards

Our awesome browser extension

Access your data through our API

**Get Privacy Personal**

# Tech Support Scam

## Don't let a tech support scammer fool you this April

- Scammers pose as tech support and request control of the victim's device.
- Victims are often told that this is necessary to remove a virus or update software
- Sign of fraud
- No legitimate tech support service should reach out proactively to ask for remote access to your computer.
- May be responding to a scary pop-up message (often the result of malware) that demands hundreds of dollars to remove a virus or resolve some other computer problem

# Tech Support Scam

**Don't let a tech support scammer fool you this April**

- Never give control of your device to anyone you don't trust
- One of the worst things you can do when it comes to cybersecurity
- You never know what happens to your device

More Information

[Fraud](#)



# Read Critically

## When in doubt, throw it out

- Take time to smell the roses and read the email or text critically
- Is the sender asking you something they wouldn't normally ask you
- Does it seem weird the credit card company is asking you to verify your information – don't they already have it?
- Are there misspelled words or unusual phrases?
- Is there a sense of urgency – respond immediately or click now.

More Information

[How To Recognize and Report Spam Text Messages | Consumer Information \(ftc.gov\)](#)





# Verify to Clarify

- Go to the company's legitimate website and log into your account to see if you have any messages

# Prescription Drug Scams

- Many older Americans are on a budget and need to save where they can
- Ad, unsolicited email, text, or social media post promises deep discounts on well-known drugs
- These drugs may be dangerous because often counterfeit drugs do not have the correct ingredients
- Give them a call
- No address? No phone number? Walk away.

More Information

[How to Protect Yourself From Online Pharmacy Scams \(aarp.org\)](https://aarp.org)



# Medicare Scams

- Spoofing calls from Medicare
- Bad actors do their homework
- Might offer to provide help with paperwork or offer medical services at a lower cost
- Real objective is to get your personal information to steal your identity and get treatment with your name, SSN, and Medicare number
  - Medicare won't call you
- Websites that look official

More Information

[How to Protect Yourself From Online Pharmacy Scams \(aarp.org\)](https://aarp.org/health/medicare/scams)



# Medicare Scams

- Spoofing calls from Medicare
- Bad actors do their homework
- Might offer to provide help with paperwork
- Objective is to get your personal information to steal your identity and get treatment with your name, SSN, and Medicare number or steal all your money
  - Medicare won't call you

More Information

[How Beneficiaries Can Prevent Medicare Fraud  
\(aarp.org\)](https://www.aarp.org)



# Medicare Scams

- Bogus websites
- Senior health fairs, robocalls, emails, texts about free medical supplies and equipment
- Medicare enrollment - Many different names calling about Medicare plans
- Hi, this is Becky, your patient advocate working closely with Medicare. Currently, Medicare is offering precautionary genetic cancer screening nationwide and has recommended that anyone over the age of 50 be tested.

More Information

[‘Becky From Medicare’ Robocall Is Sweeping the Nation \(aarp.org\)](https://www.aarp.org)



# Medicare Scams

- Hi this is Tasha and I'm calling to see if you need any help understanding your health coverage options. We have advisers ready to find gaps in your coverage or help you save money. We will call again or you can reach us directly at 1-712-823-0128. Thank you for using Insurance quotes and have a great.
- Hi, this is Jessica and I'm calling to see if you need any help understanding your health coverage options. We have adviser's ready to find gaps in your coverage or help you save money. We will call again or you can reach us directly at 1-661-735-4150. Thank you for using insurance quotes and have a great day.
- Hi this is Tori and I'm calling about your interest in receiving health insurance quotes. My team will follow up with you a call later but in the meantime you may call us at 1-801-851-1292 to get connected to a license agent. Thank you for using afford(?) health insurance plans.org and have a good.

# Medicare Scams

- *Multiple calls today to see if I need any help understanding my health coverage options. Claims to be from Insurance Quotes. I have not searched for insurance coverage, so just a cold marketing call.*
- *Call every day something about insurance but at night I will try and call back number and it does not work total scanner*
- *Repeatedly calling (Nuisance call) - Calls 2-5 times around 7am then again 2-5 times around 7pm never leaves message. Immediately calls back as soon as it goes to my voicemail. This has been happening for 3 days. Also, this number called me every day for about a week back in January.*
- One number reported coming from Orem, Utah-another one from Bakersfield, CA

# Is it a Medicare Scam?

## Phishing

- How many are receiving calls that reference you stopping by their website, and they are calling about your request for information about Medicate benefits?
- Woman called every morning at 8:11 am for 2 weeks, followed by 3 additional calls
- Occasionally calls with spoofed numbers—all numbers don't exist
- Finally stopped but started again with a man calling



# Scams

- **Charity scams.** Legitimate charities make a big push at year-end for last minute annual donations.
- Scammers know this and make their own end-of-year push to line their own pockets.
- Check the charity before donating at [charitynavigator.org](https://charitynavigator.org) or [give.org](https://give.org), and make sure your donation is going to the charities that really are using your money for good.

# Scams

- **Ukraine scams**
- Better Business Bureau and FBI have some advice about how to make sure you choose a legitimate and effective charity.
- BBB warns that scammers will likely create fake donation websites and make fraudulent pleas for money to supposedly help the people of war-torn Ukraine.
- According to the FBI, scams are prevalent after high-profile events, and “criminals often use tragedies to exploit you and others who want to help.”





More Information

[10 Tips for Donating to Charities for Ukraine](https://aarp.org/10-Tips-for-Donating-to-Charities-for-Ukraine)  
[aarp.org](https://aarp.org)



# Scams

- **Sign for those package deliveries.** Watch out for phishing scams claiming to be from UPS, FedEx and the US Postal Service asking you to click a link to solve a delivery issue.
- I hadn't ordered anything from FedEx

Fedex	Last reminder: scvjudy , please ...	   
FedEx	Last reminder: scvjudy , please respond i...	Dec 11
Fedex	Last reminder: scvjudy , please respond i...	Dec 10
Lucy	Dear Scvjudy , We Need Your Confirmatio...	Dec 10

# Scams

- **Social Security is not calling.** Scammers are spoofing the Social Security Administration's 1-800 number (which means it appears on caller ID that the actual federal agency is calling you) in order to get you to provide vital personal information.
- The AARP Fraud Watch Network was recently debriefed by the Office of the Acting Inspector General (OIG) of a new scam that is becoming more prevalent by the day. The OIG advises that scammers are spoofing caller ID to trick people into thinking that the Social Security Administration is calling. The callers then attempt to engage with the recipients and get them to provide important financial or personal information.

# Scams

- **What you should do.** If you receive a call like this, hang up.
- You can **report Social Security impostor scams to the Social Security Administration at 1-800-269-0271.**
- If you are concerned the SSA is trying to reach you, call them directly at 1-800-772-1213.
- Alert family and friends about this increasingly prevalent activity.
- Take care not to provide callers with sensitive personal or financial information such as your Social Security number or bank account information.

# Scams

- **Spoofing** involves using technology to change the number that appears on caller ID to something different.
- In this case, the calls appear to be coming from the Social Security Administration (SSA), displaying the phone number 1-800-772-1213 (the SSA's national customer service number), and the caller verbally identifies as an SSA employee.
- The typical stated reason for the call is to collect additional information to increase the person's benefit payment or to prevent benefits from being terminated.

# FCC anti-spoofing law

- Acting Chairwoman Rosenworcel and other FCC staff get spoofing calls too. As she said during one of the Commission's monthly meetings: "I'm a consumer, too. I receive robocalls at home, in my office, on my landline, on my mobile. I've even received multiple robocalls sitting here on this dais. I want it to stop."

More Information

[The FCC's Push to Combat Robocalls & Spoofing | Federal Communications Commission](#)



# FCC anti-spoofing law

- Have you noticed it is quieter in your house without the phone ringing with robocalls?
  - Went into effect on July 1, 2021
  - Standard that ensures calls that come in are actually from the number that shows up on your Caller ID
  - If phone number is spoofed, phone carriers can block the number
- Rule only affects large carriers
  - Small companies will also be required to comply
- FCC reported largest carrier implemented standard on 6/30/2021



# FCC anti-spoofing law

- Have you noticed it is quieter in your house without the phone ringing with robocalls?
  - Went into effect on July 1, 2021
  - Standard that ensures calls that come in are actually from the number that shows up on your Caller ID
  - If phone number is spoofed, phone carriers can block the number
- Rule only affects large carriers
  - Small companies will also be required to comply
- FCC reported largest carrier implemented standard on 6/30/2021

# FCC anti-spoofing law

- FCC's acting chairwoman called robocall and spoofing a top priority
- If you are still receiving robocalls, FTC suggests
  - Don't answer calls from unknown numbers
  - Hang up and call on your own if caller says they are from a company or organization
  - Hang up if you are asked to either hit a number or say yes to stop being called

# The Grandparents / Family Scam

- **How it works.** You get a frantic call from someone claiming to be your grandson or granddaughter.
- Caller says there's an emergency and asks you to send money right away.
  - Involved in a car accident
  - Need money to get out of a legal mess
- Don't act right away, no matter how dramatic the story is
- Call that family member, their parents, siblings, etc.

More Information

[Fraudsters Scam Grandparents by Posing as Grandchildren \(aarp.org\)](https://www.aarp.org/scams/fraudsters-scam-grandparents-by-posing-as-grandchildren)

# The Grandparents / Family Scam

- Set the privacy settings on your social media accounts so only people you know can access your posts and photos
- Scammers search Facebook, Instagram, and other social networks for family information they can use to fool you
- If your personal details are public, someone can use them to defraud you *and* people who care about you
- People 70 and over who sent cash reported median individual losses of \$9,000
- Losses over the past year reached \$41 million, as compared to \$26 million in the previous year

# The Grandparents / Family Scam

- Bob Gostischa got the call in 2015
    - He asked which granddaughter?
  - Caller replied: What do you mean?
    - Bob: Well, I have several
    - Caller: Your oldest
  - Caller said she was in an accident, failed the breathalyzer test, and spent the night in jail. She wanted him to wire her \$500 via Western Union.
    - Bob: Things are really tight
- More Information
- [Got an aging parent? Tell them about the Grandparent scam \(avast.com\)](https://www.avast.com/en-us/blog/grandparent-scam)



# The Grandparents / Family Scam

- Caller: Can't you put it on one of your credit cards
  - Bob: Sorry, they are all maxed out
- Caller: Please Grandpa, I don't want to stay in jail
  - Bob: Sorry sweetie, but I really can't and don't have any money I can send
- Caller: Click – she hung up.
  - His oldest granddaughter doesn't drive and would not be in Niagara Falls

# The Grandparents / Family Scam

- The United States Attorney's Office – Southern District of California
- August 25, 2021, News Release
- Eight Indicted in Nationwide Grandparent Fraud Scam, Assistant U.S. Attorney Oleksandra “Sasha” Johnson
- Defendants swindled more than \$2 million from 70-plus elderly victims across the nation, with at least eight in San Diego County.
- Scheme left many elderly victims financially and emotionally devastated
- Unconscionable to target the elderly
- First case investigated by the SD Elder Justice Task Force
- Believed to be first time Charged with violating racketeering statute = RICO

# The Grandparents / Family Scam

- If you've mailed cash, report it right away to the Postal Service or whichever shipping company you used.
- Some people have been able to stop delivery by acting quickly and giving a tracking number.
- Contact the [FTC.gov/complaint](https://www.ftc.gov/complaint). Learn more about this and other imposter scams at [FTC.gov/imposters](https://www.ftc.gov/imposters).



# Phishing Scam

- I played detective after a tech buddy asked me to look into this phishing scam.

From

microsoftsubscription46692@gmail.com

Your Purchased:

1 year Subscription

Windows Defender Advanced Threat protection Firewall & Network protection

\$499.00

Sub-total

\$499.00

Sales tax (VAT)

0.00

Discount

\$100.00

Total

\$399.00

Microsoft Account

# Phishing Scam

- Dear ,

If You didn't make this purchase or if you believe an unauthorized person is attempting to access your Microsoft account Call to our customer care representative +1 (877) 542-1879 (Toll Free).

This Email confirms payment for the Microsoft Defender listed above. You will be each plan period until you cancel by downloading to the Microsoft Defender plan from your PC.

You may contact Microsoft for a full refund within 48 Hrs. of a monthly Subscription upgrade or within 72 Hrs. after yearly payment. Partial refunds are available where required by law.

Dates are displayed per Coordinated Universal Time. Order date may vary based on your location.

Thank you for using our services

Microsoft Defender Team

Copyright @ Microsoft Corporation, One Microsoft Way, Redmond, WA  
98052 USA

# To Click or not to Click, that is the question

## A few tricks

- Configure the setting in your email account to display the sender's email address and not just their display name
- I almost fell for this one....
  - Personal address - [jlgeorge1001@aol.com](mailto:jlgeorge1001@aol.com) (not a real address)
  - Phishing email – [jlgeorge101@gmail.com](mailto:jlgeorge101@gmail.com)
  - He has both AOL and Gmail accounts
- I received the email at three of my accounts

# To Click or not to Click, that is the question

## A few tricks

- I didn't open any of the emails, this is what I started receiving at one of the accounts – up to 8 a day, down to 3 after 2 weeks and now nothing.

If you wish to unsubscribe from future mailings please click [here](#) or write to:  
4801 North Fairfax Drive Suite 1200 Arlington, VA 22203

If you wish to unsubscribe from future mailings please click [here](#) or write to:  
73 Greentree dr #80, Dover, DE 19904

If you wish to unsubscribe from future mailings please click [here](#) or write to:  
1060 Woodcock Rd Ste 128 PMB 62867 Orlando, Florida 32803-3607 US

If you wish to unsubscribe from future mailings please click [here](#) or write to:  
123 SE 3rd Ave. Suite 574, Miami, FL 33131

**Subject:** Say "Goodbye" to Blood Sugar Worries [Allow Subject](#)

**Date:** 02:34 PM PDT, 09/10/21

**From:** Diabetes News <noreply@yulagbhmgb.com> [Add to Contacts](#) [Block Sender](#)

**Subject:** Fuel Saving Device Going Viral [Allow Subject](#)

**Date:** 11:31 AM PDT, 09/10/21

**From:** Fuel Saver <noreply@mail.23andme.com> [Add to Contacts](#) [Block Sender](#)

**Subject:** Get your Timeshares approximate value for sale [Allow Subject](#)

**Date:** 08:31 AM PDT, 09/10/21

**From:** MyTimeshareExpert <noreply@mail.23andme.com> [Add to Contacts](#) [Block Sender](#)

**Subject:** Rebuild Your Gums, Teeth, and Get Rid of Tooth-Decay [Allow Subject](#)

**Date:** 08:37 AM PDT, 09/10/21

**From:** Rejuvenate Your Gums <noreply@igbgqdwtsu.com> [Add to Contacts](#) [Block Sender](#)

# **To Click or not to Click, that is the question**

**Read critically - when in doubt, throw it out**

- Don't click on links in....
  - Email
  - Tweets
  - Text
  - Posts
  - Social media messages
  - Online advertising
- DON'T Unsubscribe – you are verifying your email address and the scammers receive more money for a verified address
- Mark it as spam!

# **To Click or not to Click, that is the question**

**When in doubt, throw it out**

- Be aware of anything that comes from a stranger
- Be suspicious sent from those you don't know well

# To Click or not to Click, that is the question – Spam Folder

★ <b>Congratu</b> 📧.	<b>CHECKOUT YOUR ACCOUNT</b> 💰✅ <b>PAYOUT VERIFICATION</b> ✅💰
CA Survey Research	Final Reminder: California Opinion Survey - Dear Resident, We are an in
Surge Mastercard	Congratulations!.. Here's Your_Invitation!
Grace Nelson	Donate Charity - Greetings to you and sorry if this message came to you
Public--Records	Someone May have Run a Background-check on You,[scvjud] >
CA Survey Research	Reminder: California Opinion Survey - Dear Resident, We are an indeper
Fidelity Life	w e l c o m e - \$15/Month Buys You \$250K Term Insurance – No Medica
CA Survey Research	California Opinion Survey - Dear Resident, We are an independent public
mymortgageprofessor	Homeowners-must-read! - Banks don't want you to know this !

* <b>Roundup-L</b> 📧.	scvjud \$2 <b>billion verdict awarded in weedkiller lawsuit.</b> ..
Peoplewhiz	One Thing All Cheaters Have in Common, Brace Yourself - (2) Nega
no-reply	Confirmation:0510 - Give us your opinion about The Home Depot ar
UPS	Response Needed - Please confirm receipt
GovLoanOptions	<b>Fast Approval Refinance</b> - Check rates and calculate new pay
eharmony Info	<b>Is the right match waiting on eharmony? Find out now!</b> - Tire
Amazon	✉ scvjudy ,Your Package 📦 delivery Problem Notification ID#5704
LeafFilter Promo	Save now on the nation's best-selling gutter protection - America's
Amazon	✉ scvjudy ,Your Package 📦 delivery Problem Notification ID#892
scvjudy	\$9150.99 Deposited In Your account next day - see details - IMI

Lowe's

Verification - Lowe's reward - Open immediately!

# From the FBI

## How to Report

- If you believe you or someone you know may have been a victim of elder fraud, contact your local FBI field office or submit a tip online.
- [Phoenix — FBI](#)
- [Community Outreach — FBI](#)



### Phoenix

21711 N. 7th Street  
Phoenix, AZ 85024  
[phoenix.fbi.gov](https://phoenix.fbi.gov)  
(623) 466-1999

Covers the entire state of Arizona and Grand Canyon National Park



# From the FBI

## How to Report

- You can also file a complaint with the FBI's Internet Crime Complaint Center.
- Also file a complaint with your local police/sheriff's department

[Internet Crime Complaint Center\(IC3\) | File a Complaint](#)

# From the FBI

## How to Report

- When reporting a scam—regardless of dollar amount—include as many of the following details as possible:
- Names of the scammer and/or company
- Dates of contact
- Methods of communication
- Phone numbers, email addresses, mailing addresses, and websites used by the perpetrator

# From the FBI

## How to Report

- Methods of payment
- Where you sent funds, including wire transfers and prepaid cards (provide financial institution names, account names, and account numbers)
- Descriptions of your interactions with the scammer and the instructions you were given
- You are also encouraged to keep original documentation, emails, faxes, and logs of all communications.
- Judy's tip – create a script so you always give the same information

# FTC – [ftc.gov/complaint](https://ftc.gov/complaint)

- Report scammer to FTC – [ftc.gov/complaint](https://ftc.gov/complaint)

☐ Just an annoying call

## Report details

Please share as much as you know. The details help law enforcement investigations.

Was the call a recorded message or a robocall?

☒ Yes

☐ No

What is your phone number, or the phone number that received the call, if different?

This field is required.

What was the call about?

When did you receive the call? (mm/dd/yyyy)?

This field is required.

Have you done business with this company in the last 18 months or contacted them in the last 3 months?

☐ Yes

☐ No

