



# Cybercriminals are after us

Lorain County Computer User Group

June 13, 2023

# Brought to you by....

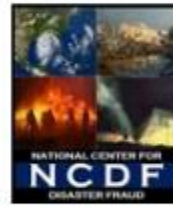
- APCUG's Speakers Bureau, a benefit of your group's membership in APCUG
  - Judy Taylour, President, SCV Computer Club
- APCUG Advisor – Regions 10, 11, and International
  - jtaylour (at) apcug.org



# Consumer Sentinel Network – 2023 Report



FEDERAL TRADE COMMISSION  
PROTECTING AMERICA'S CONSUMERS





# A Scammy Snapshot of 2022

(based on reports to Consumer Sentinel)

#FTCTopFrauds  
ftc.gov/data  
ReportFraud.ftc.gov

## Top Frauds



**2.4 million** fraud reports



**\$8.8 billion** reported lost

The number of reports is down.  
The amount lost is up.  
(2021: 2.9 million fraud reports, \$6.1 billion lost)

Losses to investment scams more than doubled.



**\$1.8 billion**

2021

**\$3.8 billion**

2022

Losses to business imposters soared.



**\$196 million**

2020

**\$453 million**

2021

**\$660 million**

2022

Scammers contacting people on social or by phone led to big losses



**\$1.2 billion** total lost

**Social media:** Highest overall reported losses



**\$1,400** median loss

**Phone calls:** Highest per person reported losses

# Consumer Sentinel

- Unique investigative cyber tool that gives members of the Consumer Sentinel Network access to millions of reports.
- Reported fraud losses are up
- Imposter scams top Fraudulent Five
- Losses to business imposters have skyrocketed
- Investment scams are on a troubling upswing
- Scammers go social

# 2022 Fraud Results

CONSUMER  
SENTINEL  
NETWORK  
DATA BOOK 2022

SNAPSHOT

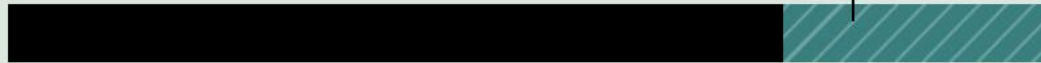
5.2  
MILLION  
REPORTS

## TOP THREE CATEGORIES

- 1 Identity Theft
- 2 Imposter Scams
- 3 Credit Bureaus, Info Furnishers and Report Users

2.4 million fraud reports

26% reported a loss



\$8.8 billion total fraud losses | \$650 median loss

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

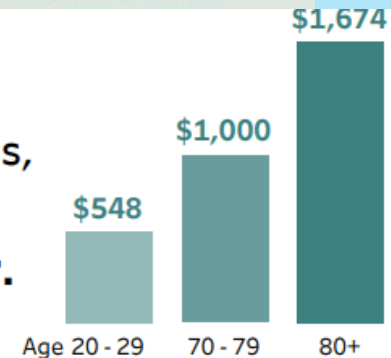
43%

Age 20-29

23%

Age 70-79

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



# 2022 Fraud Results

## Imposter Scams




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

\$2.667 billion  
reported lost  
\$1,000 median loss

## Identity Theft Reports

13% 

Credit card new  
account fraud

88% 

Government  
Benefits Applied  
For\Received

# 2022 Report Categories

## Report Categories

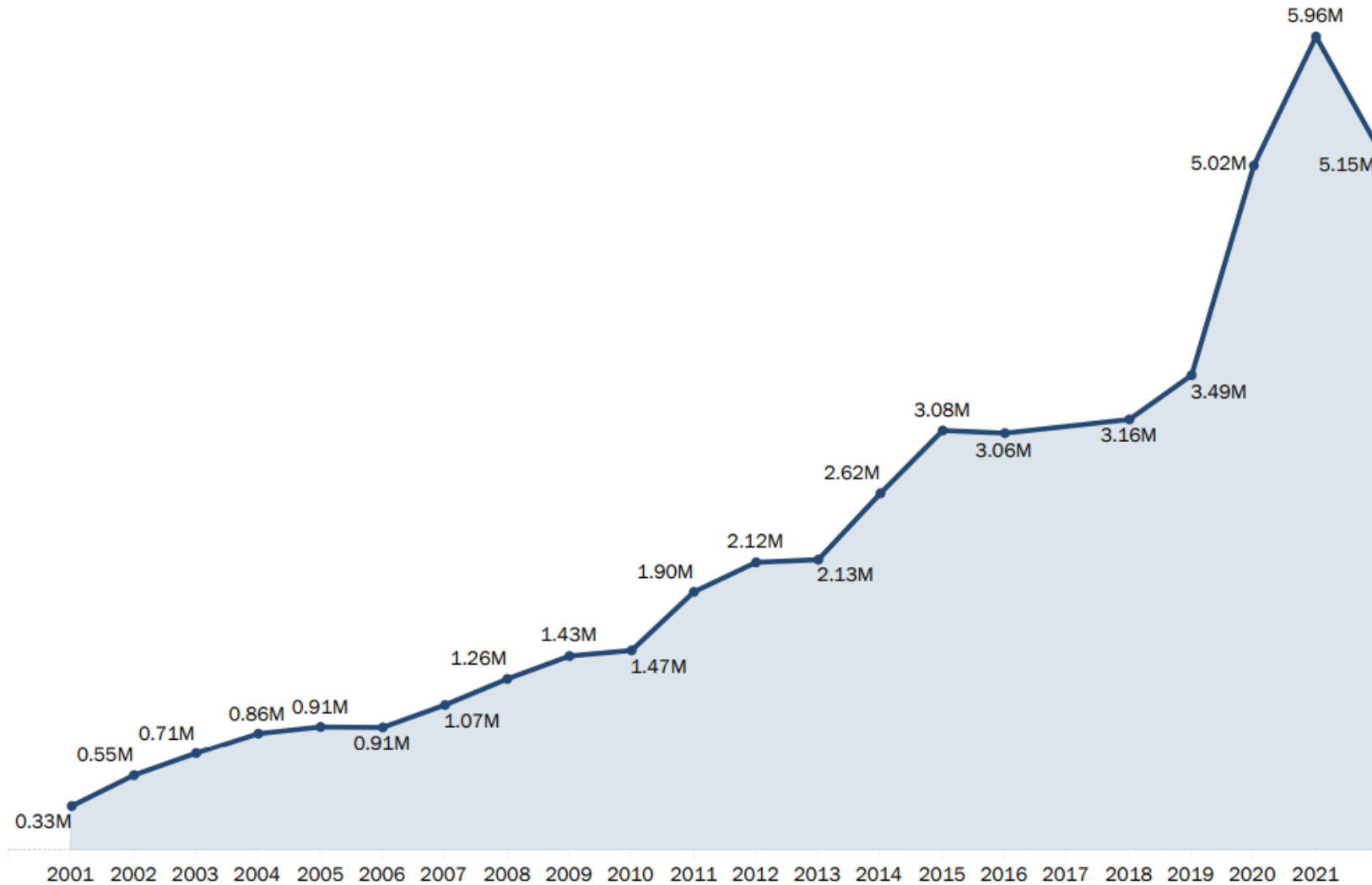
Rank	Category	# of Reports	%
1	Identity Theft	1,108,609	21.52%
2	Imposter Scams	725,989	14.10%
3	Credit Bureaus, Information Furnishers and Report Users	691,142	13.42%
4	Online Shopping and Negative Reviews	327,609	6.36%
5	Banks and Lenders	249,126	4.84%
6	Auto Related	162,040	3.15%
7	Prizes, Sweepstakes and Lotteries	143,132	2.78%
8	Debt Collection	112,827	2.19%
9	Internet Services	110,189	2.14%
10	Investment Related	104,703	2.03%
11	Health Care	99,370	1.93%
12	Business and Job Opportunities	95,399	1.85%
13	Telephone and Mobile Services	89,376	1.74%
14	Credit Cards	87,451	1.70%
15	Home Repair, Improvement and Products	82,482	1.60%

16	Privacy, Data Security, and Cyber Threats	66,383	1.29%
17	Travel, Vacations and Timeshare Plans	62,445	1.21%
18	Foreign Money Offers and Fake Check Scams	40,903	0.79%
19	Television and Electronic Media	35,515	0.69%
20	Advance Payments for Credit Services	34,558	0.67%
21	Mortgage Foreclosure Relief and Debt Management	24,037	0.47%
22	Education	19,690	0.38%
23	Computer Equipment and Software	16,912	0.33%
24	Charitable Solicitations	9,958	0.19%
25	Tax Preparers	7,116	0.14%
26	Magazines and Books	6,073	0.12%
27	Office Supplies and Services	4,040	0.08%
28	Grants	2,419	0.05%
29	Funeral Services	1,470	0.03%



# 2022 Fraud Results

Number of Fraud, Identity Theft and Other Reports by Year



# 2022 Fraud Loss Payment

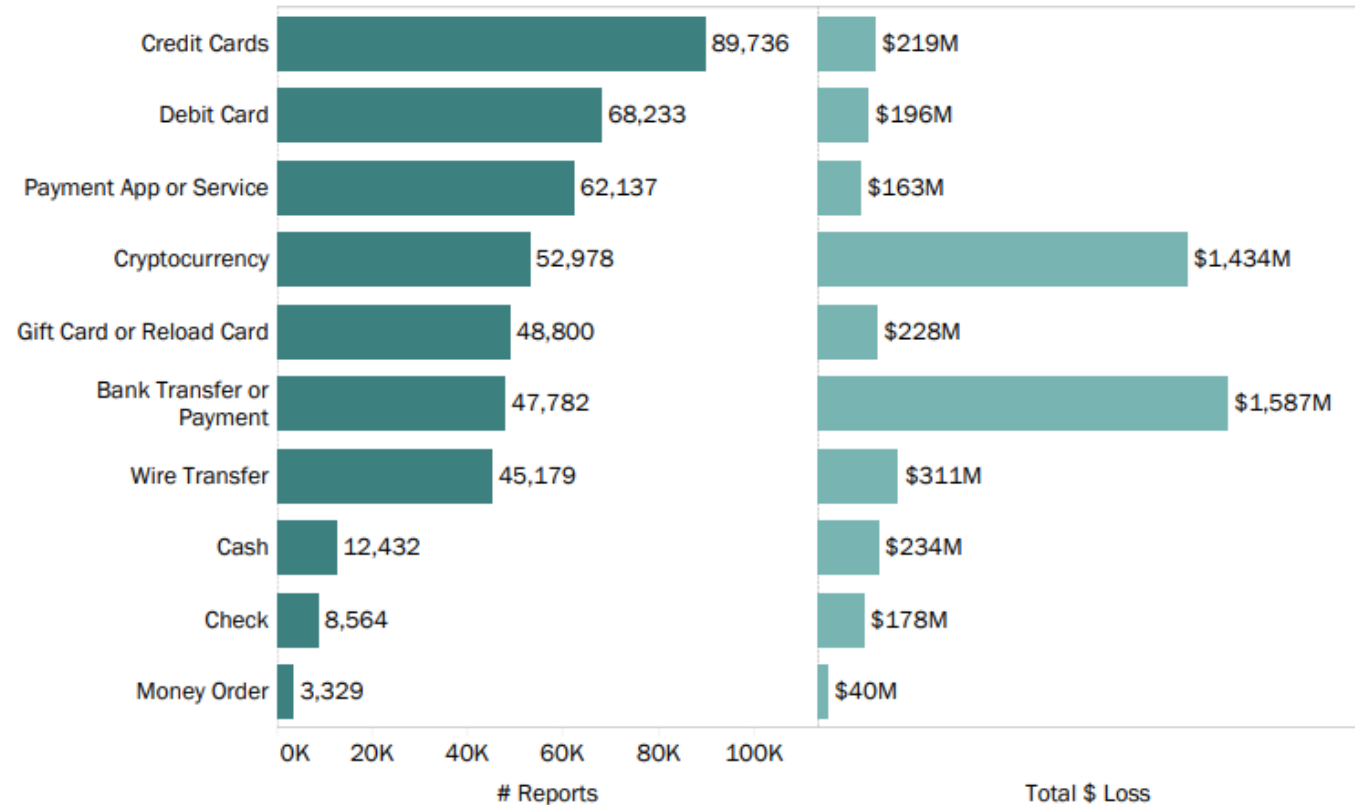
## Fraud Reports by Payment Method

2,369,527

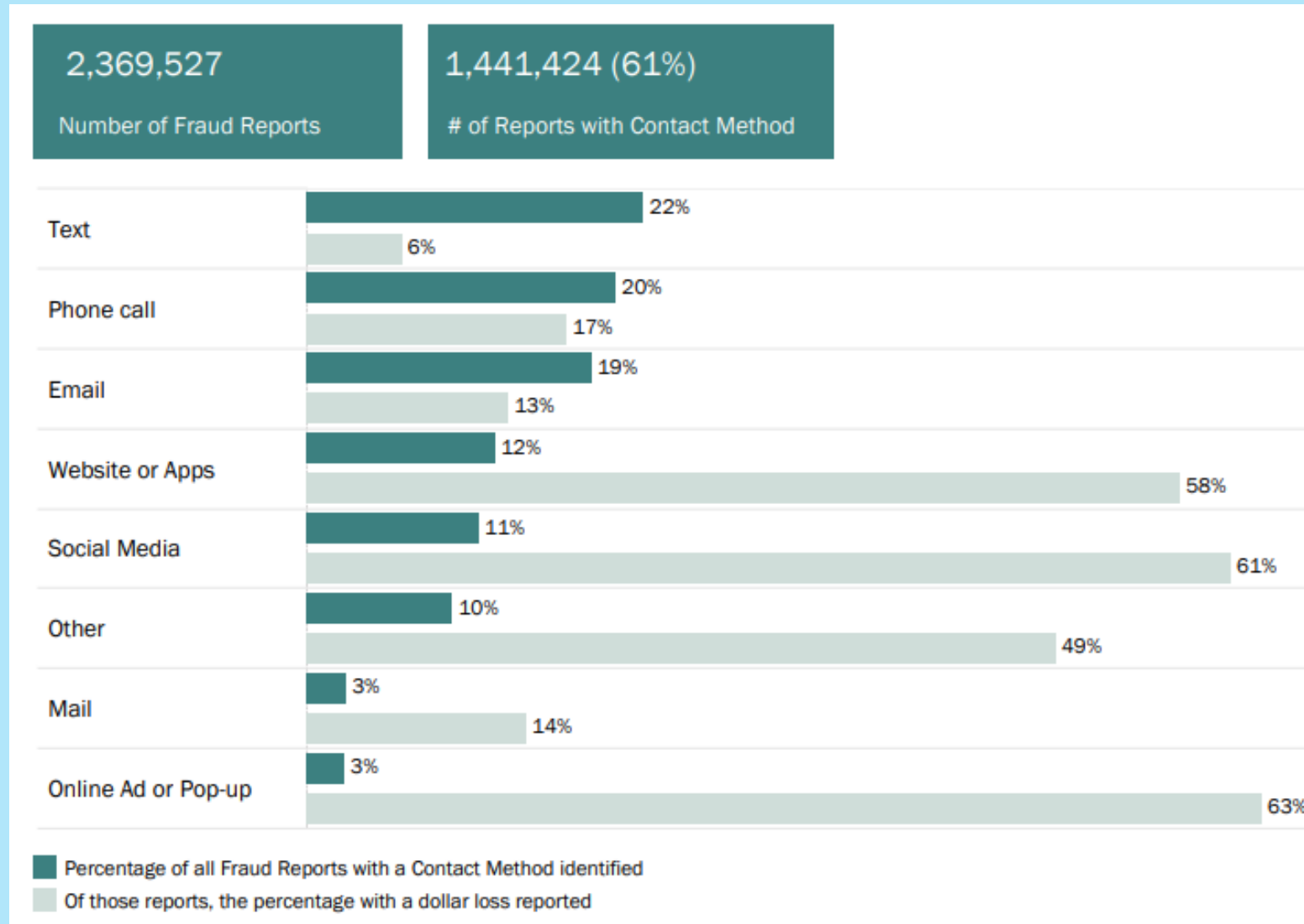
Number of Fraud Reports

439,170 (19%)

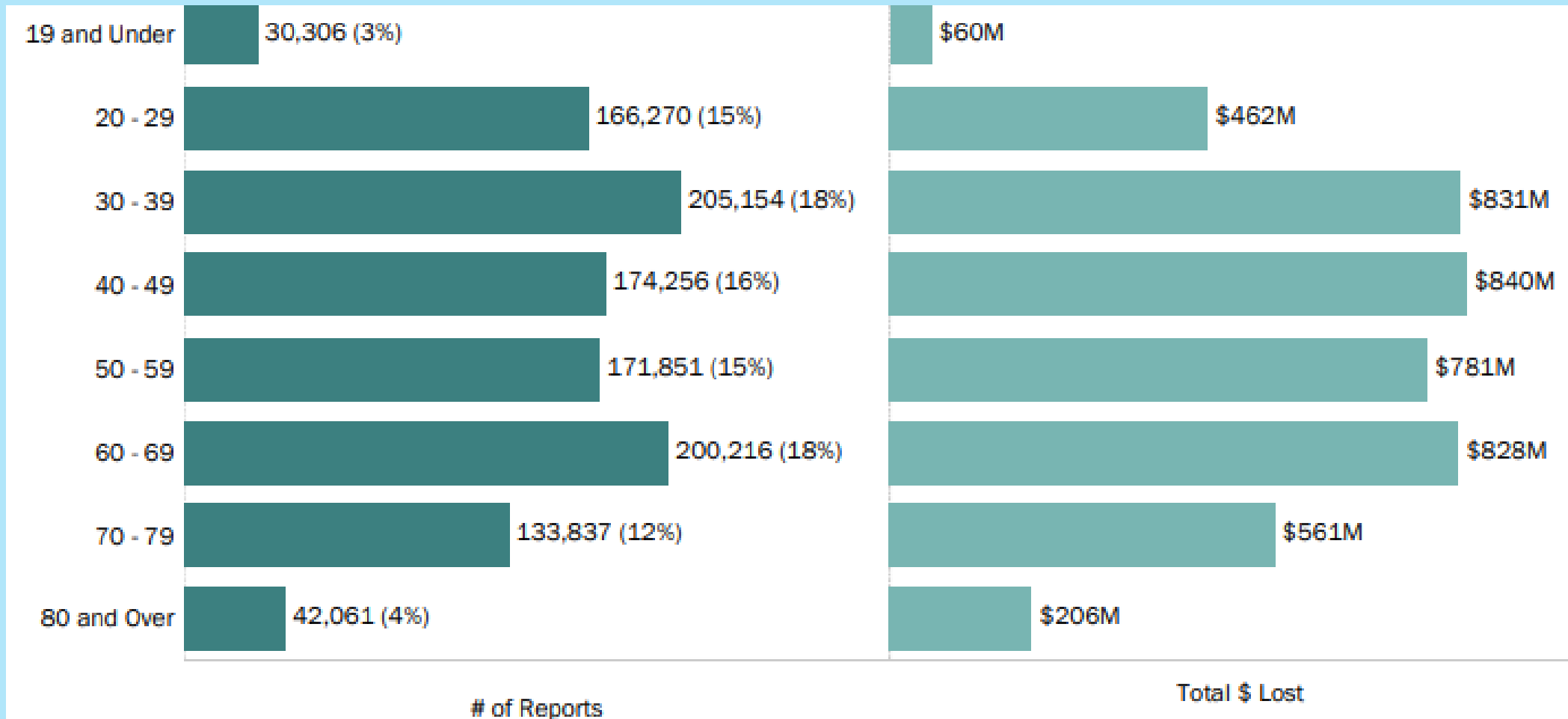
# of Reports with Payment Method



# 2022 Fraud Contact Method

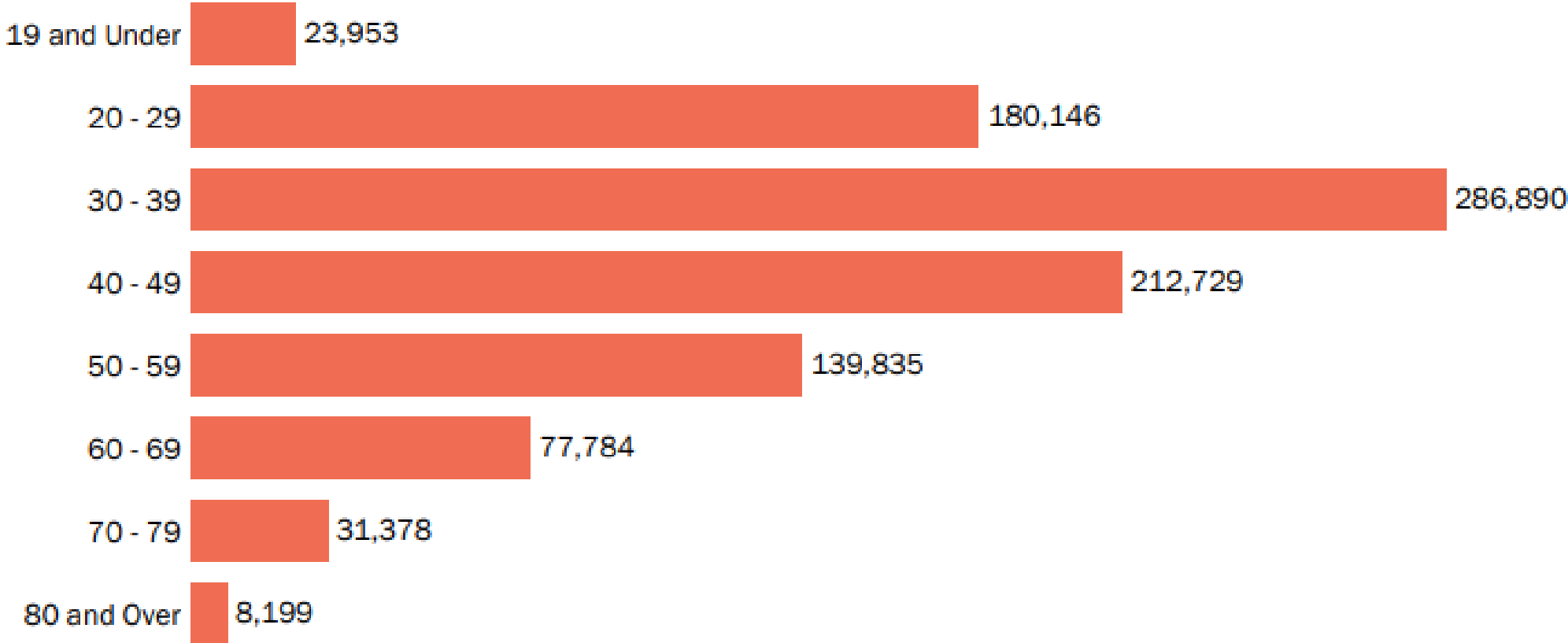


# 2022 Fraud Loss by Age



Percentages are based on the total number of 2022 fraud reports in which consumers provided their age: 1,123,951.

# 2022 ID Theft by Age



# 2022 Fraud & ID Theft State Ranking

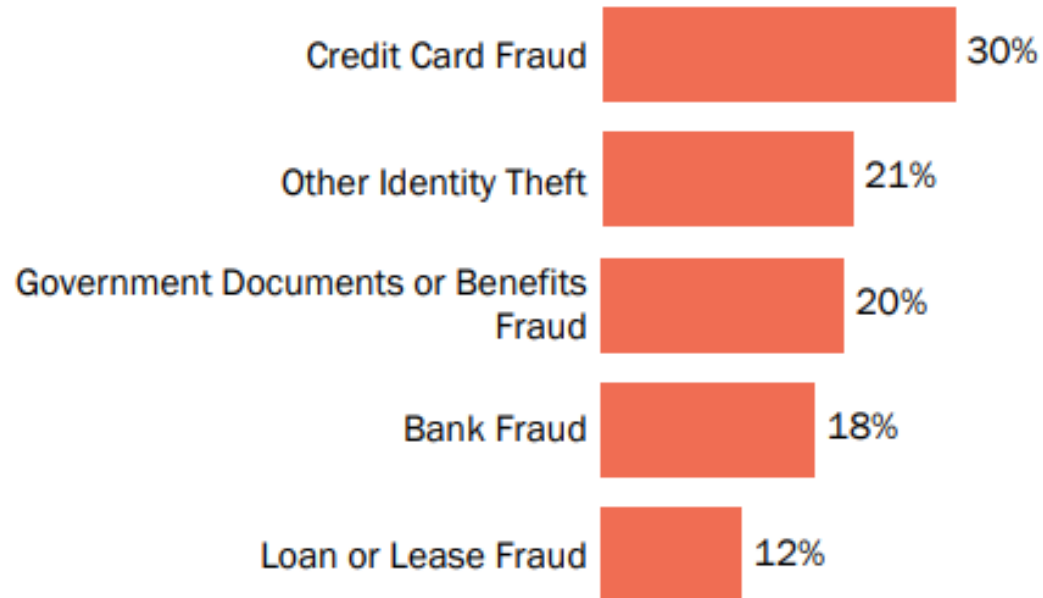
## Ohio

Rank	State	Reports per 100K Population	# of Reports
10	New Jersey	1,070	95,073
11	Tennessee	1,063	72,011
12	North Carolina	1,060	110,090
13	Arizona	1,051	75,407
14	Colorado	1,051	59,746
15	Texas	1,028	294,378
16	Illinois	1,017	129,325
17	New York	974	190,101
18	California	947	372,800
19	Louisiana	946	44,137
20	Washington	936	70,297
21	Oregon	927	38,703
22	Missouri	923	56,535
23	Connecticut	900	32,140
24	Michigan	893	89,025
25	Ohio	886	103,419
26	Massachusetts	878	60,325

Rank	State	Reports per 100K Population	# of Reports
1	Georgia	574	60,348
2	Louisiana	534	24,898
3	Florida	524	111,221
4	Delaware	484	4,682
5	Nevada	418	12,672
6	Texas	397	113,808
7	Pennsylvania	368	47,143
8	Alabama	363	17,763
9	South Carolina	352	17,908
10	Mississippi	344	10,260
11	Maryland	343	20,736
12	Illinois	335	42,558
13	New Jersey	323	28,712
14	California	319	125,597
15	New York	312	60,835
16	North Carolina	304	31,609
17	Arizona	265	19,018
18	Ohio	265	30,950
19	Virginia	261	22,177
20	Tennessee	238	16,124

# 2022 ID Theft Types - Ohio

## Top Identity Theft Types



## Identity Theft Reports

18th

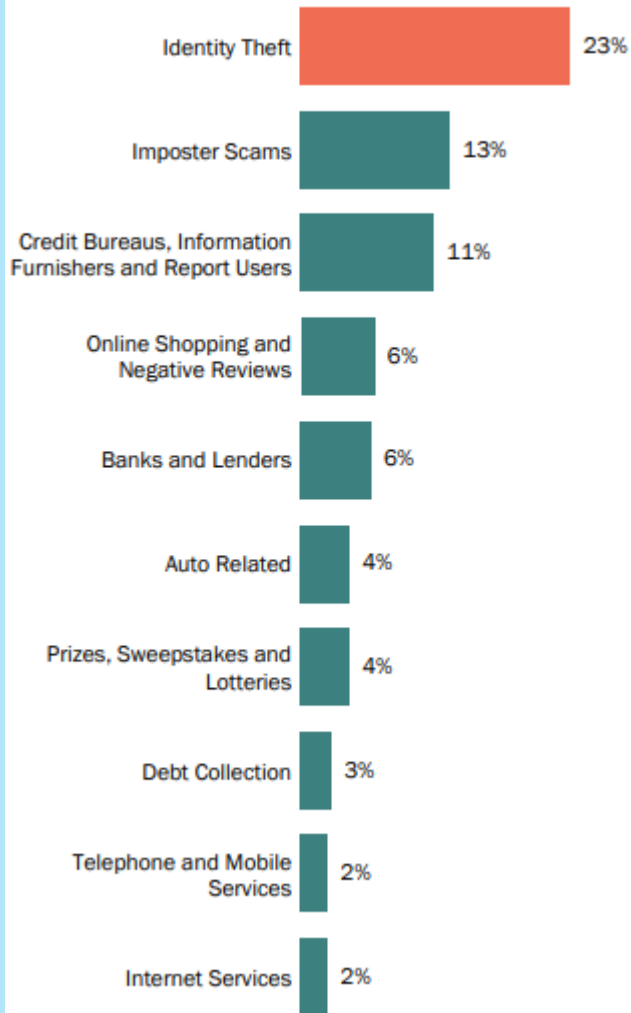
State Rank  
(Reports per 100K Population)

30,950

Identity Theft Reports

# 2022 Fraud & Other Reports - Ohio

## Top Ten Report Categories



## Fraud & Other Reports

25th

State Rank  
(Reports per 100K Population)

103,419

Total Fraud & Other Reports

## Fraud Losses

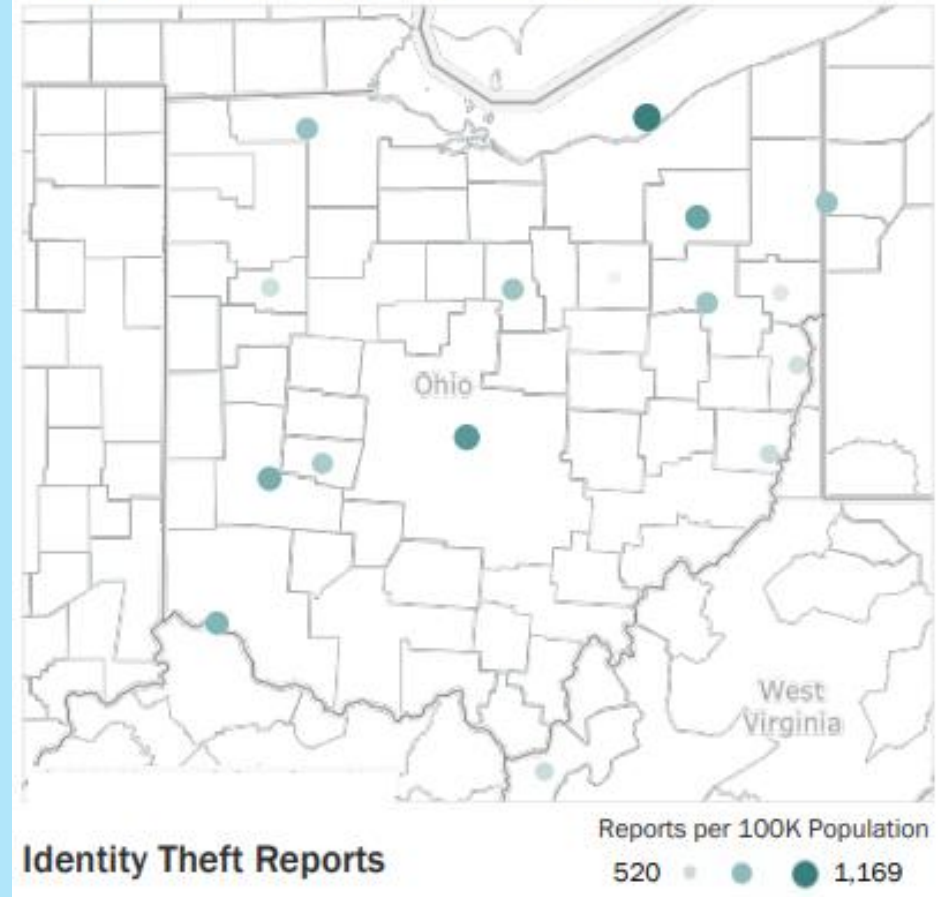
\$135.3M

Total Fraud Losses

\$500

Median Fraud Losses

## Fraud & Other Reports by Metropolitan Area





# 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
- Funeral 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
- Investment Fraud
- Market Manipulation (Pump and Dump) Fraud
- Money Mules
- Nigerian Letter or “419” Fraud
- Non-Delivery of Merchandise

# From the FBI

## Common Elder Fraud Schemes – a long list

- Online Vehicle Sale Fraud
- Ponzi Schemes
- Pyramid Schemes
- Ransomware
- 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://www.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 \(ftc.gov\)](#)



FEDERAL TRADE COMMISSION  
**CONSUMER ADVICE**

# 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://www.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://www.aarp.org/what-to-do-if-a-ransomware-attacks-your-computer)



# Ransomware 101

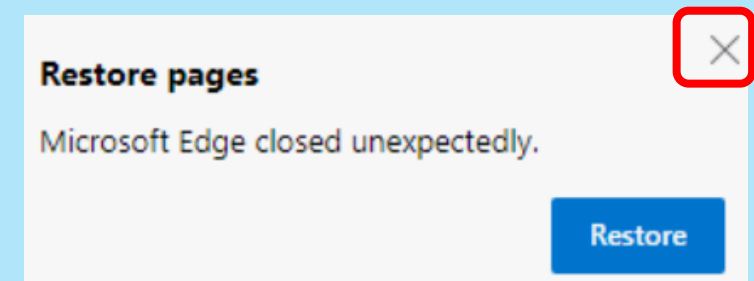
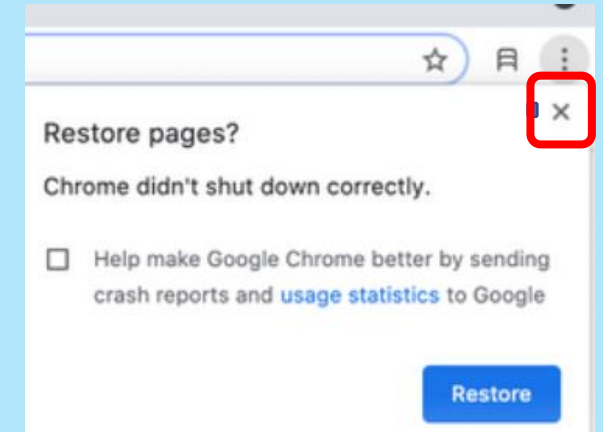
## How do you get it?

- 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

# Ransomware 101

## What should you do?

- Use Alt+F4 to close the open window or pop-up
- Take a picture on your screen
- Shut down your computer
- Turn it back on (reboot)
- Don't click on Restore pages when you open your browser
- See if you can access your files
- If yes
  - Do a deep scan with your anti-virus program
  - Run Malwarebytes



# 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.
- If you have a picture, add it to your complaint
- 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 \(ftc.gov\)](#)



FEDERAL TRADE COMMISSION  
CONSUMER ADVICE

# 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

# 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 \(ftc.gov\)](#)



FEDERAL TRADE COMMISSION  
CONSUMER ADVICE

# 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://www.aarp.org/health/medication/2017/06/01/how-to-protect-yourself-from-online-pharmacy-scams/)



# 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://www.aarp.org/health/medicare/2017/06/01/online-pharmacy-scams/)



# 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)



# 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 Medicare 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](http://charitynavigator.org) or [give.org](http://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://www.aarp.org/10-tips-for-donating-to-charities-for-ukraine)  
([aarp.org](https://www.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

# 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)

# 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

# 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-scams)



# 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

# 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

# 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).



# Spooftng

- **Spooftng** involves using technology to change the number that appears on caller ID to something different.
- 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 & Spooftng | 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

# Government Agencies

- Won't call, email, or text you to verify personal details
  - Social Security, bank account, or credit card numbers
- Won't ask you to pay by cryptocurrency, gift card, money transfer, or cash
- Won't threaten you if you don't pay
  - Social Security
  - IRS
  - DEA
  - Jury Duty
  - Outstanding warrant

# Who isn't going to call you

- Microsoft about your computer = how would they know
- ??? company about your computer's security

# One-ring scam call

- Scammers use three initial digits that resemble U.S. area codes
- 232 goes to Sierra Leone and 809 goes to the Dominican Republic
- Don't call back -- risk being connected to a phone number outside the U.S.
- May end up being charged a fee for connecting, along with significant per-minute fees for as long as they can keep you on the phone.
- Before calling unfamiliar numbers, check to see if the area code is international.
- If you do not make international calls, ask your phone company to block outgoing international calls on your line.

# One-ring scam call

## One-ring scam call

- If billed for a call you made as a result of this scam
- Try to resolve the matter with your telephone company.
- If you are unable to resolve it directly, file a complaint with the FCC at no cost.



# Oldie but Goodie

## Check Washing is alive and well

- Do you leave your mail in an 'open' mailbox?
- Do you have bad actors in your area that break into locked mailboxes?
- Check washing is soaring due to pandemic
  - Government stimulus checks
  - Unemployment checks
- Looking for new sources of income
- Sell washed checks to other criminals for \$250 - \$600 each
- Can also sell account holders' SSNs and size of bank balance

# Oldie but Goodie

## Check Washing is alive and well

- Sell bank account and routing numbers used to withdraw funds electronically

## How to prevent check washing

- Use online banking and electronic bill pay forms of Bill Pay as a more secure way to pay
- Use a blue or black non-erasable gel pen
  - Gel seeps into the fibers of a check and will ruin a washing attempt

# Oldie but Goodie

## How to prevent check washing

- Don't use stand-alone USPS mailboxes
  - Scammers can “fish” for mail by dropping a string with a sticky substance on the end into the receptacle and pulling envelopes out
- Never raise the red flag on the box
  - An invitation for criminals to take your mail over other boxes where the flag is down
- Monitor bank accounts / Report incidents within 30 days
  - Banks are generally required to replace funds stolen by fraudulent checks if reported within 30 days.

# Oldie but Goodie

## How to prevent check washing

- Monitor bank accounts / Report incidents within 30 days
  - Banks are generally required to replace funds stolen by fraudulent checks if reported within 30 days.
- Contact US Postal Inspection Service and credit reporting agencies

[Security Center - Fairfield County Bank](#)

[6 Steps You Should Take to Stop Check Washing \(aarp.org\)](#)

[Report Mail Fraud & Postal Fraud | USPIS](#)

# USPS Informed Delivery

## See Photos of Your Mail Before It Arrives, Free

- Start your mornings with a preview of your day's USPS<sup>®</sup> mail and packages with Informed Delivery<sup>®</sup> notifications
  - Daily Digest emails that preview your mail and packages scheduled to arrive soon
  - Images of your incoming letter-sized mail (grayscale, address side only)
  - Track and manage your packages in one convenient place
- [Informed Delivery - Mail & Package Notifications | USPS](#)

# 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

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

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

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

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

**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](#)

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

**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](#)

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

**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@igbgqdwtu.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!

This is an advertisement. This message has been sent to you through an affiliate of Renewal by Andersen.

To be removed from receiving future emails, [Unsubscribe here.](#)

If you have questions or concerns, contact our customer support team, [here.](#)

2040 Merrick Road Unit 408 Merrick, NY 11566



# **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

Delete forever | Not spam | 1-1 of 1 < >

Messages that have been in Spam more than 30 days will be automatically deleted. [Delete all spam messages now](#)

<input checked="" type="checkbox"/> ☆	<b>Erick Andrew</b>	<b>Read &amp; Understand</b> - Did you receive the email I sent you concerning Brian.	9:41 PM
<input checked="" type="checkbox"/> ☆	<b>Reagan Broadcast</b>	<b>World Athletics Takes Controversial Stance On Transgender Athletes</b> - And First Biden Came After Your S...	4:15 AM
<input type="checkbox"/> ☆	<b>Lawsuit Claims</b>	<b>Notifications</b>	9:41 AM
<input type="checkbox"/> ☆	<b>BioLyfe CBD</b>	<b>Confirmation receipt 59455</b>	8:49 AM
<input type="checkbox"/> ☆	<b>YourAutoSavings</b>	<b>WelcomeToYourAutoSavingsInsurancekaF</b>	8:27 AM
<input type="checkbox"/> ☆	<b>Endurance</b>	<b>Welcome to Endurance Auto 2742</b>	6:41 AM

# Think Before...

You click on a link

Email

Social Media site (Facebook, Twitter...)

Website/pop-ups

\*\*\*\*\*

Answer the phone


Respond to a text / SMS message

# 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.

<https://www.fbi.gov/contact-us/field-offices/cleveland/about>

 **Stay Connected** Get FBI email alerts

[Subscribe](#)

[No Thanks](#)



## Main Field Office Territory

**Counties covered:** Cuyahoga and Lorain

# 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)

## 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



