



Cybercriminals are after us

Seniors Computer User Group of Greater Kansas City

March 11, 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



Checked my Facebook page after the presentation



William James

6m · 🌐

Dear friends, my apologies, but I was hacked in Messenger which sent a message 'Look who died' to everyone in my contact list. I would advise you change your password in FB as I have. I received that message from a friend who I knew and we both knew of someone that was ill. I clicked on the link without checking first as to the validity of the message. My sincere apologies for any inconvenience that this may have caused. I should have known better. --- Bill J.



Santa Clarita Valley Sheriff's Station

3h · 🌐

Have you ever received an email from an account like PayPal or Amazon warning of suspicious activity on your account, asking you to log in to unlock your account? Wait right there! Most of the time, these emails are scammers trying to get you to log in to steal your information. Here's a tip: by clicking on the sender's name, it will reveal the email ID used to send the alert, showing an email not affiliated with any type of support or customer service. Don't be quick to c... See more



From: **PayPal Support**

To: >

Yesterday at 5:36 PM

**Click Here
To Verify
Sender**

Account Locked



Dear

Your account has been limited. We have found suspicious activity on your last transaction.

Login to your PayPal and verify your identity. Your PayPal account will remain limited until you complete the steps requested.

[Login to PayPal](#)

Sincerely,

PayPal Support

👍 40

3 Comments 5 Shares

👍 Like

💬 Comment

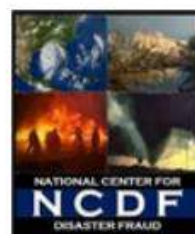
➦ Share



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% 

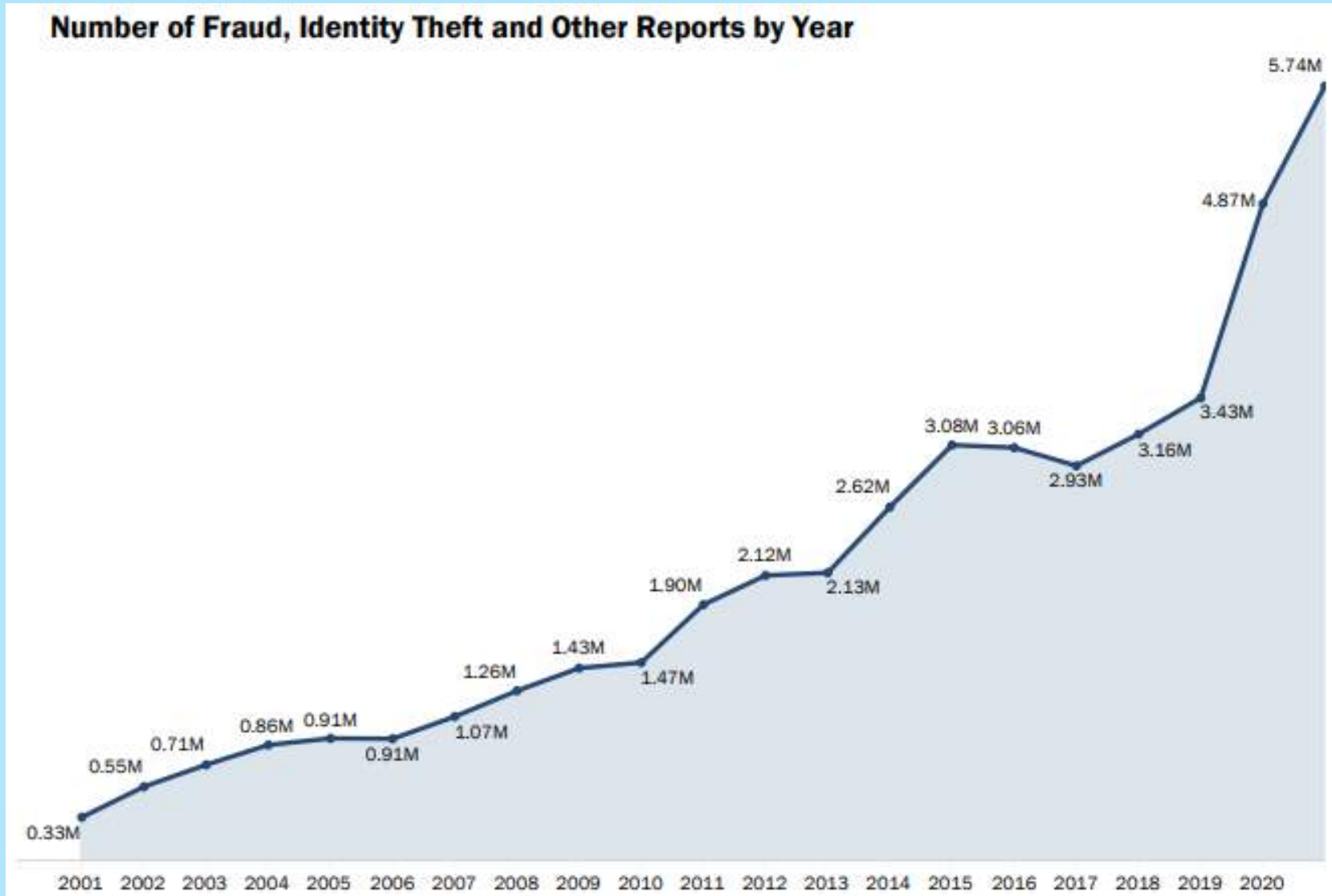
Checking\Savings
Account - New

22% 

Mobile
Telephone –
New Accounts

FEDERAL TRADE COMMISSION • ftc.gov/data

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

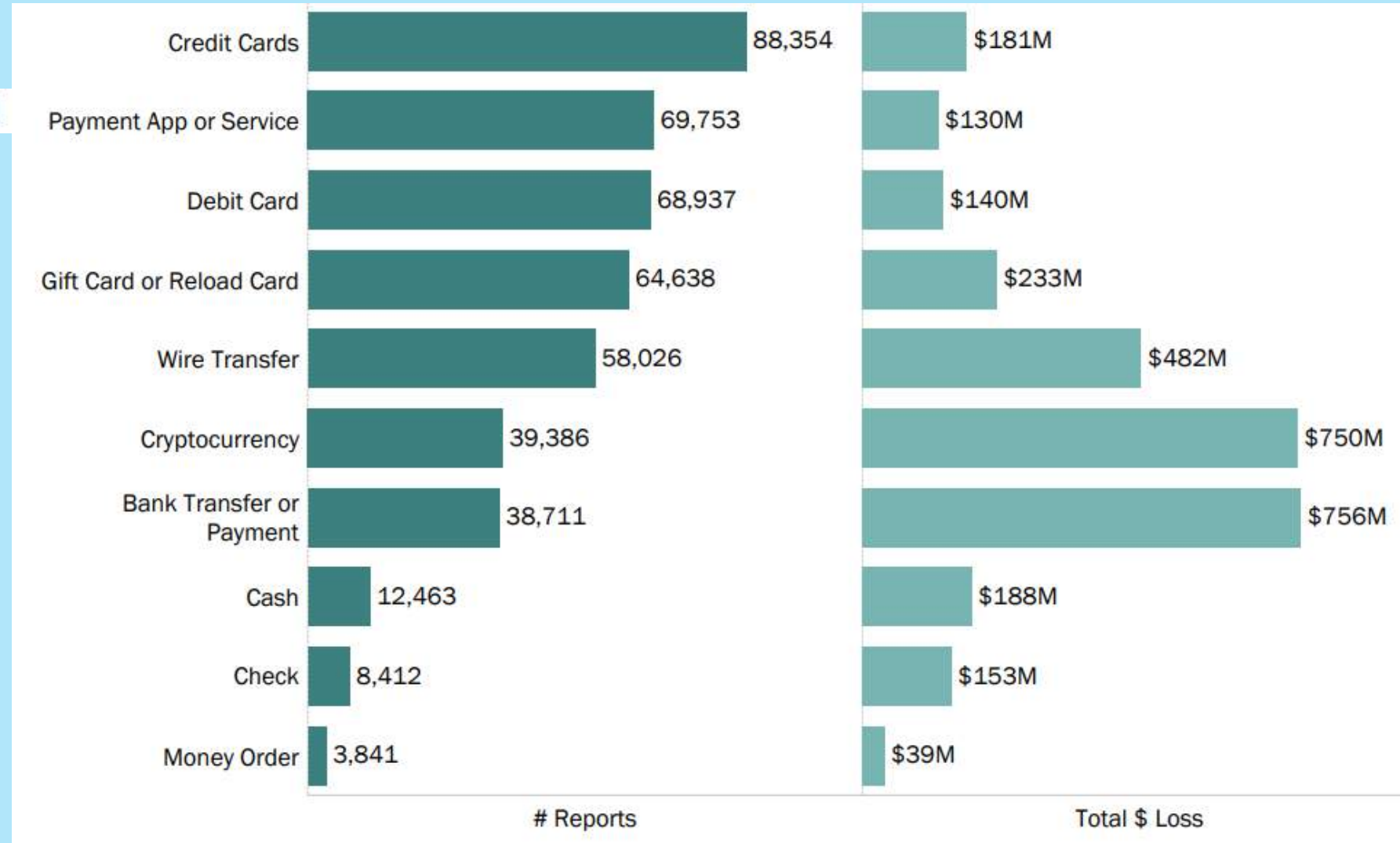
Amount Lost	# of Reports
\$1 - \$1,000	447,732
\$1,001 - \$2,000	74,179
\$2,001 - \$3,000	35,101
\$3,001 - \$4,000	19,743
\$4,001 - \$5,000	16,112
\$5,001 - \$6,000	9,425
\$6,001 - \$7,000	6,804
\$7,001 - \$8,000	6,034
\$8,001 - \$9,000	4,215
\$9,001 - \$10,000	7,496
More than \$10,000	65,535

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

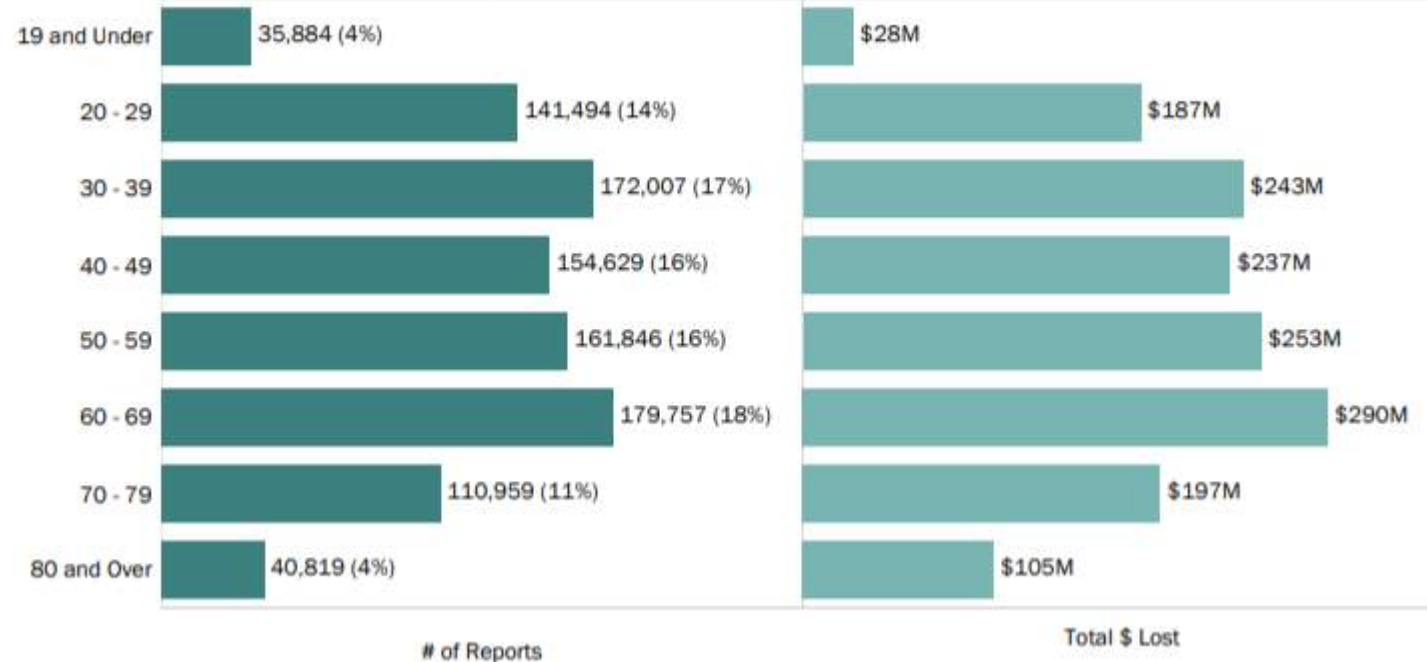


2021 Fraud Results

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.

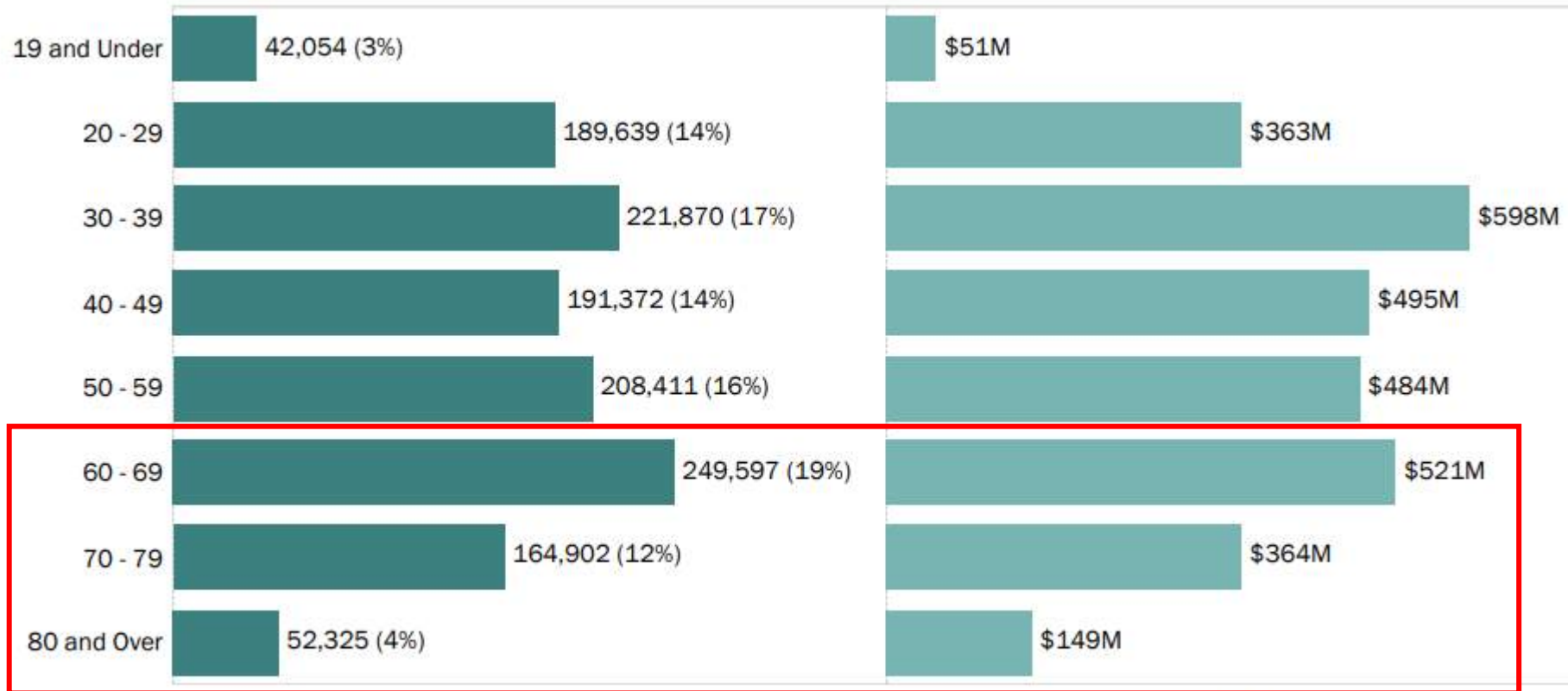
2021 Fraud Results

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



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

2021 Fraud Results

State Rankings: Fraud and Other Reports

Rank	State	Reports per 100K Population	# of Reports
27	Connecticut	917	32,686
28	New Hampshire	914	12,429
29	Mississippi	906	26,958
30	New Mexico	888	18,613
31	Michigan	881	87,996
32	Indiana	861	57,988
33	Hawaii	851	12,051
34	Vermont	848	5,292
35	Kansas	845	24,615
36	Utah	823	26,373
37	Maine	821	11,035

State Rankings: Identity Theft Reports

Rank	State	Reports per 100K Population	# of Reports
1	Rhode Island	2,857	30,270
2	Kansas	1,355	39,461
3	Illinois	924	117,056
4	Louisiana	732	34,043
5	Georgia	618	65,666
6	Nevada	584	17,985
7	Colorado	583	33,572
8	New York	563	109,466
9	Delaware	560	5,449
10	Florida	515	110,675

Kansas

Top Ten Report Categories



2021 Fraud Results

Fraud & Other Reports

35th

State Rank
(Reports per 100K Population)

24,615

Total Fraud & Other Reports

Fraud Losses

\$19.9M

Total Fraud Losses

\$429

Median Fraud Losses

Top Identity Theft Types



Identity Theft Reports

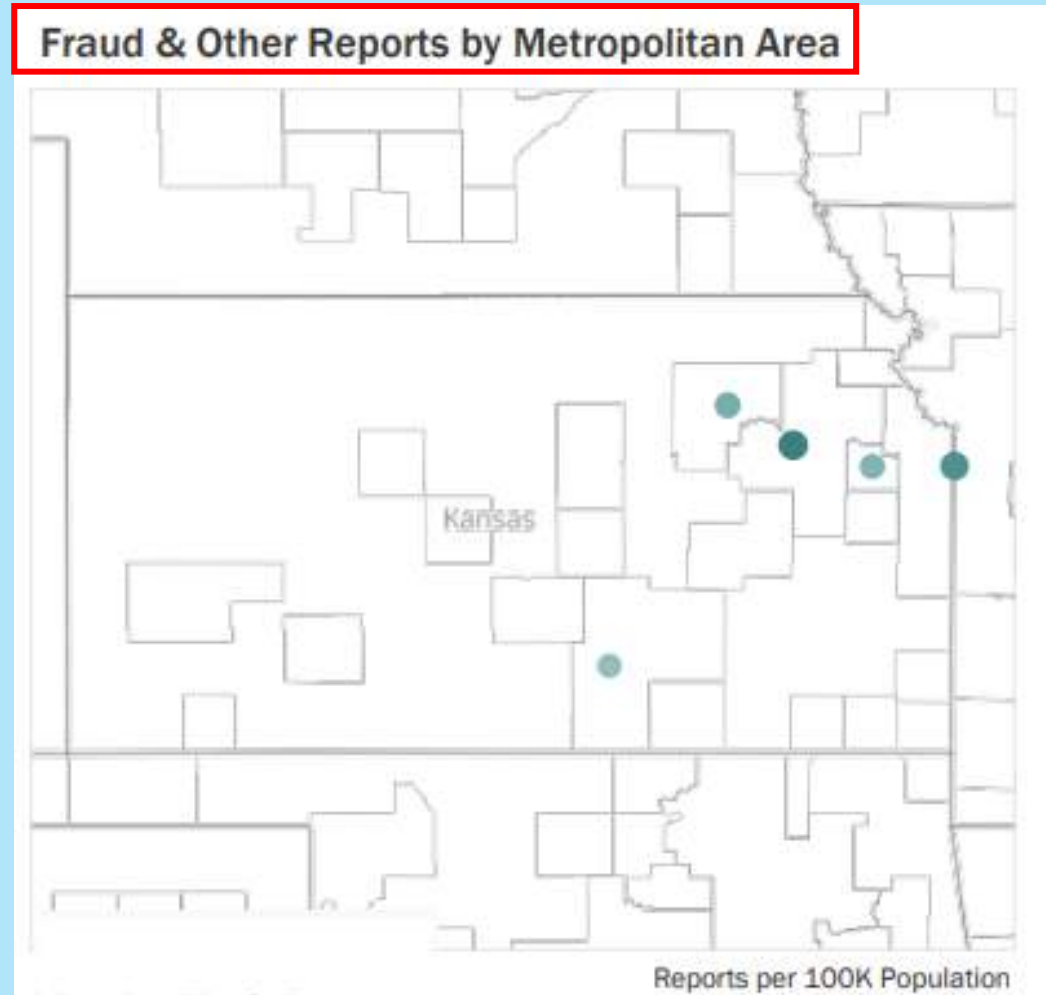
2nd

State Rank
(Reports per 100K Population)

39,461

Identity Theft Reports

2021 Fraud Results



Stalkerware

- Stalkerware apps can allow someone to track anything you do on your device.
- Partner, ex-.....
- Can track
 - Location
 - Phone calls
 - Viewing text messages and emails
- 80% of domestic violence shelters surveyed are working directly with survivors who were tracked via GPS
- 75% report abusers eavesdropped on their conversation using hidden mobile apps

Stalkerware

Protect yourself from Stalkerware

- Don't leave your device unattended
- Lock your device
- Only download apps from official app stores
- Create strong passphrases only you would know
- Review downloaded apps
- Use anti-virus software

Stalkerware

Detecting Stalkerware

- For iOS users:
- Go to your settings app
- Scroll to the bottom to see a list of all downloaded apps
- *To check which apps have access to your camera, microphone and location, go to **Settings -> Privacy for complete lists of** apps that have access to your camera, microphone, location and other features.*

Stalkerware

Detecting Stalkerware

- For Android users:
- Go to your settings app
- Select Apps & Notifications -> See All Apps
- *To check which apps have access to your camera, microphone*
- *and location, go to **Settings** -> **Privacy** -> **Permission***
- ***Manager for complete lists of apps that have access to your camera, microphone, location and other features.***

Stalkerware

Detecting Stalkerware

- If you find Stalkerware on your device
- Do a factory reset
- Get a new device
- Change login credentials

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

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

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

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
- Alt+F4 should close the pop-up or shut down your computer

Ransomware 101

What should you do?

- If you did Alt+F4 or shut down your computer and find 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

Money Mule

Happens in several ways

- Online dating, work-at-home job, prizes
- Scammers send money to you, sometimes by check
- Ask you to send (some of) it to someone else
- Often want you to use gift cards or wire transfer
- Don't tell you money is stolen
- Lying about reason for sending it
- Scammers check may clear
- Later turn out to be a fake check

Money Mule

Happens in several ways

- You deposit the check and are asked to open an account at another bank and deposit the money in that account
- 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.

Money Mule

Happens in several ways

- Or, you are asked to deposit in your account
- Open an account in another institution
- Transfer the money to that account
- Give scammer new account information
- Scammer ends up with the money
- You may have participated in money laundering

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 review 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 3rd party payment service
 - PayPal, Google Pay, Apple Pay
- Do they really need all your information they are asking for?
- Check your bank and credit card statements

Prescription Drug Scams

- Fraudsters place ads or email seniors about prescription drugs that cost far less than their normal pharmacy charges.
- Many older Americans are on a budget and are desperate to save where they can.
- They may be taken in by this scam, which is dangerous because often counterfeit drugs do not have the correct ingredients, will not help their condition, and are designed simply to make money.

Medicare Scams

- Most seniors are eligible for Medicare, but the costs may still be high for some out-of-pocket expenses.
- Fraudsters will contact older people to provide help with paperwork or offer medical services at a lower cost, but their real objective is simply to get their hands on their personal information (like social security number) to steal their identity and their life savings.
- Spoofing calls
- Websites

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 everyday 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*

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.
- Called every morning at 8:11 am for 2 weeks, followed by 3 additional calls
- Occasionally calls with spoofed numbers, no more 3 calls after his







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 or give.org, and make sure your donation is going to the charities that really are using your money for good.

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

- 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
- 2020 people received about 4B robocalls a month – FTC
- 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

FCC anti-spoofing law

- Acting Chairwoman Rosenworcel and other FCC staff get these 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."

The Grandparents / Family Scam

- **How it works.** You get a frantic call from someone claiming to be your grandson or granddaughter. The caller says there's an emergency and asks you to send money right away. But there's a good chance this is an imposter trying to steal your money through the "grandparent scam."
- Scammers usually claim to be in a desperate situation, such as being involved in a car accident or needing money to get out of a legal mess. The caller poses as your grandchild, or a law enforcement officer or attorney calling on your grandchild's behalf – whatever it takes to sound convincing.

The Grandparents / Family Scam

- People 70 and over rarely report to the FTC that they paid a scammer with cash.
- But for one particular type of fraud – family and friend imposters – fully 25% of people 70 and over reported to the FTC that they sent cash.
- People 70 and over report that the scammer posed as a grandchild, usually a grandson, about 70% of the time.

The Grandparents / Family Scam

- People from all age groups reported median individual losses of about \$2,000 to family and friend imposters – far higher than the median loss of \$462 reported to us this year for all fraud types.
- People 70 and over who sent cash reported median individual losses of \$9,000.
- Aggregate losses to family and friend imposters have increased.
- Losses over the past year reached \$41 million, as compared to \$26 million in the previous year.

The Grandparents / Family Scam

- Don't act right away, no matter how dramatic the story is.
- Call that family member or friend, and make sure you use a phone number that you know is right.
- Or check it out with someone else in your circle, even if the caller told you to keep it a secret.
- Be careful about what you post on social media.
- If your personal details are public, someone can use them to defraud you *and* people who care about you.

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 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
- Caller: Can't you put it on one of your credit cards

The Grandparents / Family Scam

- 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
- From *Got an aging parent? Tell them about the Grandparent scam*

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

SoCal Edison Warns Customers About ‘Caller ID Spoofing’ Scam

- SoCal Edison has reported an increase in “Caller ID Spoofing” a practice where scammers can falsify the caller ID on cell and home phones.
- “We have recently experienced an increase in reports of caller ID spoofing,” said Mike Marelli vice president, business customer division.
- Calls may appear to be from SCE, when in reality, the caller has no association with SCE and may try to sell you products, collect personal information or say your electric bill is past due when it’s not, said Marelli.
- The power company advises customers to never give out your personal information, such as your SCE account number, Social Security number, Tax ID, credit card information or PIN number.

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 (not a real address)
 - Phishing email – 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@yulagbhmgmb.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@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

★ Congratu💎.	CHECKOUT YOUR ACCOUNT💰✅PAYOUT VERIFICATION✅💰
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 !

To Click or not to Click, that is the question

Public--Records	Someone May have Run a Background-check on You,[scvjud] >>View
Public--Records	Someone May have Run a Background-check on You,[scvjud] >>View
ZDNet	The best mobile app development bootcamps - VPNs for iPhones; Fitness tr
Freedom__Financial_	Debt__solutions_are___here - When do negotiations begin?
*Roundup-L💎.	scvjud \$2 billion verdict awarded in weedkiller lawsuit. are you
Peoplewhiz	One Thing All Cheaters Have in Common, Brace Yourself - (2) Negative item
no-reply	Confirmation:0510 - Give us your opinion about The Home Depot and we'll g
UPS	Response Needed - Please confirm receipt
GovLoanOptions	Fast Approval Refinance - Check rates and calculate new payments.

To Click or not to Click, that is the question

* Roundup-L 📌.	scvjud \$2 billion verdict awarded in weedkiller lawsuit.
Peoplewhiz	One Thing All Cheaters Have in Common, Brace Yourself - (2) Nega
no-reply	Confirmation:0510 - Give us your opinion about The Home Depot an
UPS	Response Needed - Please confirm receipt
GovLoanOptions	Fast Approval Refinance - Check rates and calculate new pay
eharmony Info	Is the right match waiting on eharmony? Find out now! - 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

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.

[Kansas City — FBI](#)

- Each field office is overseen by a special agent in charge

Garden City, KS - Manhattan, KS - Topeka, KS - Wichita, KS

Jefferson City, MO - Joplin, MO - St. Joseph, MO –

Springfield, MO

