



# Santa Clara County District Attorney's Office

---

## Senior Fraud Prevention





---

Presented by:

Joe Burdick

District Attorney Investigator

Santa Clara County District Attorney's Office

- Financial Elder Abuse Unit
- Financial Abuse Specialist Team Member



# The Problem

---

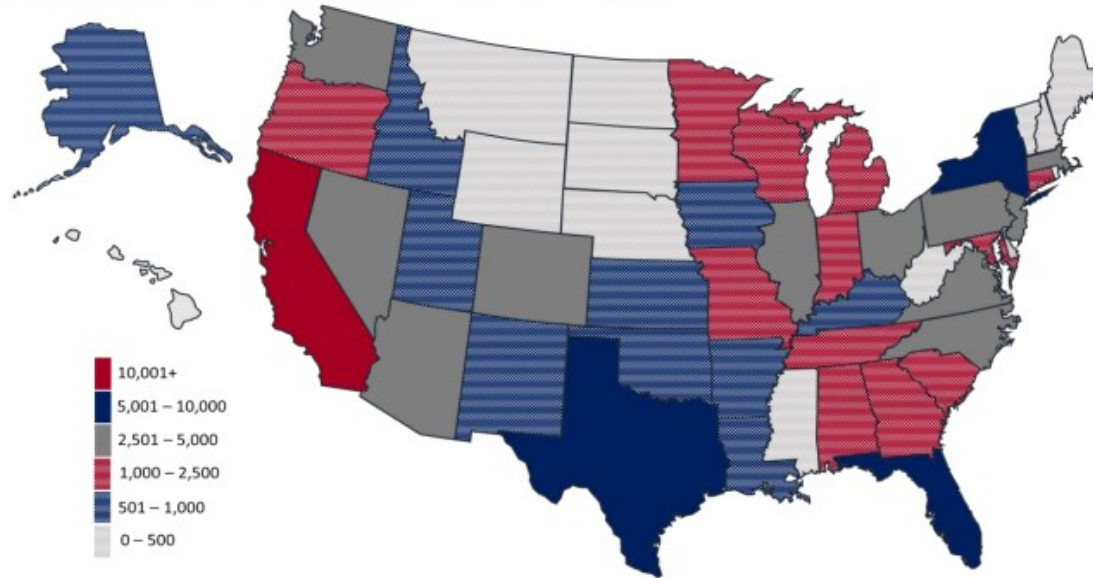


The number of elder fraud victims had been on the rise and jumped by 54.8% in 2020, although it came down in 2021. Losses, on the other hand, have been rapidly climbing every year. From 2017 to 2021, **losses were up by 391.9%**.

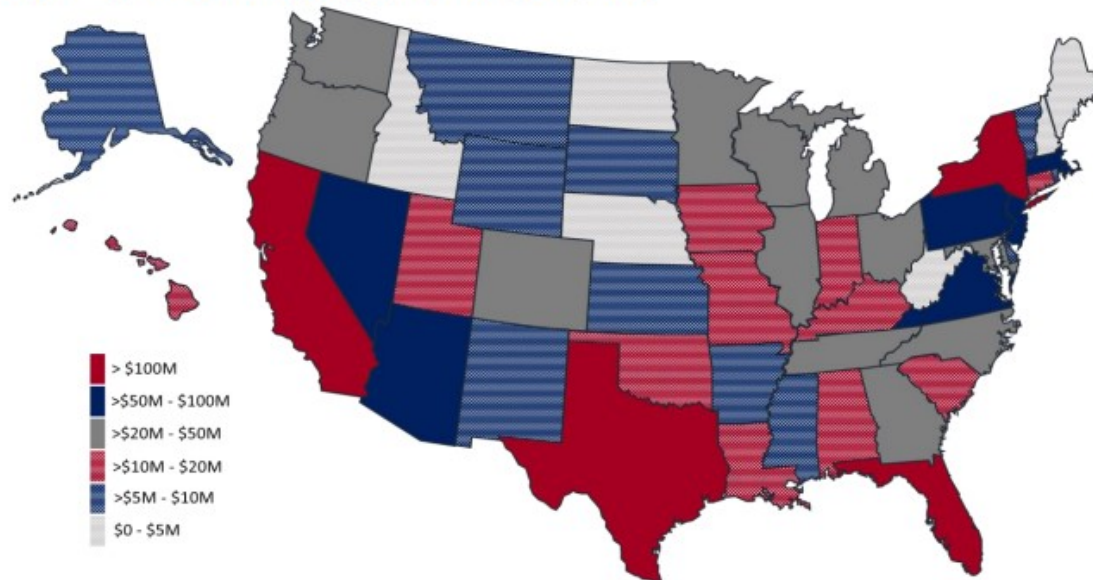
YEAR	NUMBER OF ELDER FRAUD VICTIMS	TOTAL LOSSES
2017	49,523	\$342,531,972
2018	62,085	\$649,227,724
2019	68,013	\$835,164,766
2020	105,301	\$966,062,236
2021	92,371	\$1,685,017,829

*Data source: Federal Bureau of Investigation (2022).*

2021 – STATES BY NUMBER OF OVER 60 VICTIMS<sup>4</sup>



2021 – STATES BY LOSSES OF OVER 60 VICTIMS




WHAT IS  
"ELDER  
FINANCIAL  
ABUSE?"

- **\*60 years or older**
- **Use or acquisition of an elder's money or assets contrary to the elder's wishes, needs or best interests**
- **For the abuser's personal gain**
- **Reasonably knowing that the victim is an elder or dependent adult**



## WHY TARGET ELDERS?

- **They've had more time to build wealth than younger adults and could have substantial assets, such as properties, savings, and retirement accounts.**
  - **Some are more vulnerable due to the effects of aging and health issues.**
  - **Some live alone and are more trusting in strangers due to loneliness.**
  - **They may not want to report fraud because of embarrassment, or because they fear being considered unable to manage their own finances**
- 

TYPE OF ELDER FRAUD	NUMBER OF VICTIMS (2021)	TOTAL LOSSES (2021)
Confidence fraud/romance	7,658	\$432,081,901
Business email/email account compromise	3,755	\$355,805,098
Investment	2,104	\$239,474,635
Tech support	13,900	\$237,931,278
Personal data breach	6,189	\$103,688,489
Real estate/rental	1,764	\$102,071,631
Government impersonation	3,319	\$69,186,858
Identity theft	8,902	\$59,022,153
Lottery/sweepstakes/inheritance	2,607	\$53,557,330
Non-payment/non-delivery	13,220	\$52,023,580
Credit card fraud	3,164	\$39,019,072
Advanced fee*	3,029	\$36,464,491

*Data source: Federal Bureau of Investigation (2022). \*Money paid in anticipation of receiving greater value, but less than expected or nothing is received.*

# Top Scams Targeting Seniors

# Business Imposters / Phishing E-Mail

Your Updates NIBHX93630717024 ⌵ Inbox x



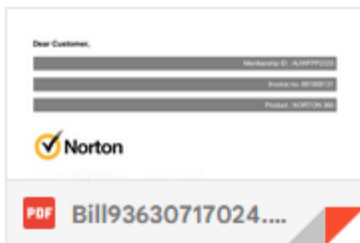
**Billing Department5603990** <angelojames7436@gmail.com>

to me ▾

Hey jburdick190

To determine when to renew, please refer to the attached file Bill881909131.

**One attachment** • Scanned by Gmail ⓘ



Dear Customer,

Membership ID : AUWFPP2333

Invoice no- 881909131

Product : NORTON 360



Hello, jburdick190@gmail.com

We are pleased to inform you that the payment for renewing your Norton membership has been received.

Features : Norton 360 offers production for up to 3 PC or Mac

Date : February 23, 2023

Duration : 2 Years

### "Billing Details"

Payment Mode : Auto Renewal

Amount : 231.35 USD

Tax : 0.00 USD

**Total : 231.35 USD.**

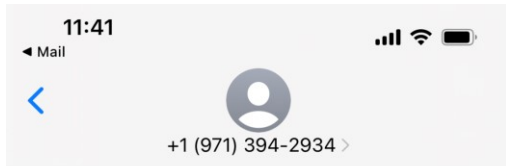
Need Help? In case there is anything unclear or if you have any questions, feel free to call us at [+1\(866\)-525-7746](tel:+1(866)525-7746)

Note: This is an automated mail. Please don't reply. If you have any concerns, kindly contact our support team directly.

**Thanks & Regards**  
Norton



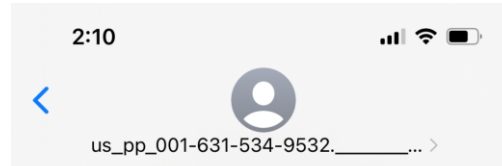
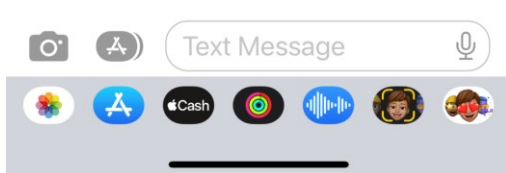
# Business Imposters / Text Messages



Text Message  
Today 11:40 AM

We have shipped your package LS906021, and charged your account for \$1808. If you have any questions or need assistance, please contact us at [+18445849493](tel:+18445849493)

The sender is not in your contact list.  
[Report Junk](#)



Sun, Jan 22 at 10:36 AM

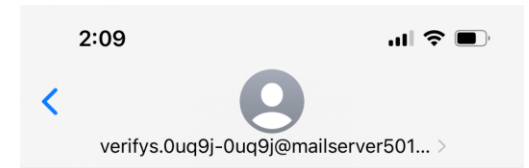
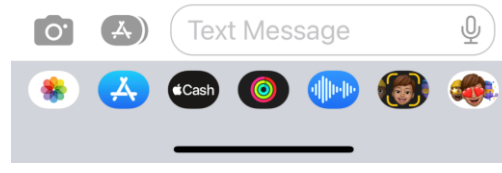
As a security check against your PayPal account has been restricted.

Please click on the following link to provide your information: <https://safelinks.ffm.to/limited-pp10032us>

If we do not receive a response to our verification attempt within the next 24 hours, we will permanently limit your account.

Thank you,  
PayPal

The sender is not in your contact list.  
[Report Junk](#)

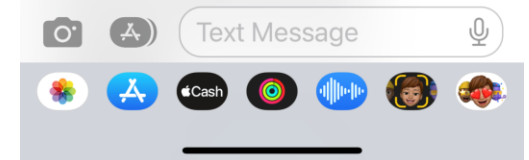


From: Account-Amazon Notification  
Msg: We have discovered an issue with your billing information. Please review your information carefully.. ID#XZVARLCAKV You're only required to follow the steps to recover your account:

1. Sign in to your account.
2. Follow the step to see your case.
3. Resolve the problem by completing the instruction.

Update Information Here :  
<https://luck356.cfd/V6BqzIA>

You can't access your



# Business Imposters / Tech Support / Payment Service

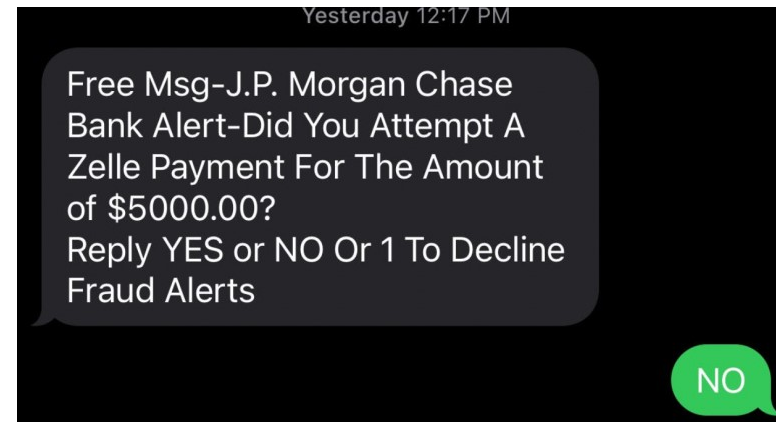
"Before I get into the details, I need to verify that I'm speaking to the right person. What's your username?"

**In the background, they're using the username with the forgot password feature, and that's going to generate two-factor authentication passcodes.**

"I'm going to send you the password and you're going to read it back to me over the phone."

The scammer then uses the code to complete the password reset process, and then changes the victim's online banking password. The fraudster then uses Zelle to transfer the victim's funds to another account

Scammers never even need to know or phish the victim's password



# Tech Scam



## WARNING!

**SYSTEM MAY HAVE DETECTED  
VIRUSES ON YOUR COMPUTER**

System May Have Found (2) Malicious Viruses: *Rootkit.Skelf.Spy* and *Trojan.FakeAV-Download*. Your Personal & Financial Information **MAY NOT BE SAFE.**

**For Help Removing Viruses, Call Tech Support Online Right Away:**

**1(855) 970-1892**  
(TOLL-FREE, High Priority Call Line)

Your IP Address: [REDACTED] Generated on 02-18-2014 | Priority Support



**WARNING!**

**YOUR COMPUTER MAY BE INFECTED:**

System Detected (2) Malicious Viruses: *Rootkit.Skelf.Spy* and *Trojan.FakeAV-Download*. Your Personal & Financial Information **MAY NOT BE SAFE.**

**To Remove Viruses, Call Tech Support Online Now:**

**1(866) 627-4049**  
(TOLL-FREE, High Priority Call Line)



```
0x0000000E DRIVER_UNLOADED_WITHOUT_CANCELLING_PENDING_OPERATIONS
WINDOWS HEALTH IS CRITICAL
DO NOT RESTART
PLEASE CONTACT WINDOWS TECHNICIANS

BSOD : Error 333 Registry Failure of
operating system - Host :
BLUE SCREEN ERROR 0x000000CE


Please contact Windows technicians At Toll Free : 1-844-354-5941
To Immediately Rectify Issue to prevent Data Loss
```


Call center making fraudulent calls in Bangalore, India.







# In The News

 An official website of the United States government [Here's how you know](#) ▾

 DOJ Menu

 **United States Attorney's Office**  
Eastern District of Virginia

[About EDVA](#) | [Find Help](#) | [Contact Us](#)

Search 

[About](#) ▾ | [News](#) | [Services & Programs](#) ▾ | [Careers](#) | [Contact Us](#)

[Justice.gov](#) > [U.S. Attorneys](#) > [Eastern District of Virginia](#) > [Press Releases](#) > [Leader of International Robocall Scam Sentenced for Defrauding Over 4,000 U.S. Victims Out of More Than \\$10 Million](#)

## PRESS RELEASE

# Leader of International Robocall Scam Sentenced for Defrauding Over 4,000 U.S. Victims Out of More Than \$10 Million



Thursday, September 16, 2021

Share >

### For Immediate Release

U.S. Attorney's Office, Eastern District of Virginia

RICHMOND, Va. – An Indian national was sentenced today to 22 years in prison for conspiracy and identity theft in connection with his operation of an overseas robocall scam that defrauded thousands of victims out of more than \$10 million.

“This defendant has been sentenced to 22 years in prison for being the mastermind and leader of an extensive multimillion-dollar robocall scheme that, from overseas, exploited over 4,000 American victims,” said Raj Parekh, Acting U.S. Attorney for the Eastern

- IRS/Treasury Department scam calls / texts – the IRS or Treasury Department **will not contact you by phone if you are late or have not paid taxes.** These are impostors!



# Government Imposters



# Sweepstakes / Lottery Scams

The initial contact in a sweepstakes scam is often a **call, an email, a social media notification or a piece of direct mail** offering congratulations for winning some big contest.

**But there's a catch:** You'll be asked to **pay a fee, taxes or customs duties to claim your prize.** The scammers may request your bank account information, urge you to send money via a wire transfer, or suggest you **purchase gift cards** and give them the card numbers.



BABCOCK, JACOB A <babcoj@email.sc.edu>

Mon 1/27/2020 10:40 AM

BABCOCK, JACOB A; BABCOCK, JACOB A ▾



**CONGRATULATIONS!!**

*Your email was selected in Powerball Lottery Draw with the sum of 1.5million dollars .kindly send your Full Name,Address and phone number for claims*

*Yours Sincerely  
Mr James Walter  
Head of Operations*

# Romance Scams

Signs of Romance Fraud,  
Indicators that you have  
fallen for a scam; (1)



- **Professes Love Quickly**, Soul Mate, lifelong relationship
- Claims to be from the United States but is **overseas for business**, offshore oil rig or military service.
- Meets you on a dating site but quickly has you **move to a site like WhatsApp, WeChat, Telegram**.
- Promises to meet in person, but there are always excuses. Those excuses quickly turn to **financial excuses**.



# Types of Money Mules

## Unwitting or Unknowing

- Individuals are unaware they are part of a larger scheme
- May be told to keep a portion of the money they transferred
- Motivated by trust in the actual existence of their romance or job position

## Witting

- Individuals ignore obvious red flags or act willfully blind
- May have been warned by bank employees they were involved with fraudulent activity
- Open accounts with multiple banks in their true name

## Complicit

- Individuals are aware of their role and actively participate
- Travel, as directed, to different countries to open financial accounts or register companies
- Recruit other money mules
- Motivated by financial gain or loyalty to a known criminal group

# HOW TO AVOID FINANCIAL ABUSE

Most scams rely on older **victims panicking, becoming flustered, or making hasty decisions.**

- **STOP:** Take a moment and think about the situation. Does anything feel suspicious?
- **LEAVE: Hang up, close the door, delete the text, or close the email.** If someone is pressing you to act now, they could be a con artist.
- **ASK:** Call a family member for advice, search online for more details, and find out if the organizations you're speaking to are real. You can also ask a visitor for identification.
- **WAIT:** Take the time to absorb what you've learned and make a plan of action. **Don't rush any decisions.**
- **ACT: Only visit legitimate websites and call verified, safe phone numbers.** You can use independent review websites and email address lookup services to check someone's identity.

# REPORTING

All Fraud can always be reported to Adult Protective Services in your area. [1-800-414-2002](tel:1-800-414-2002)

- through the mail, report to the USPIS
- on the internet, FTC at [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud)
- on the phone, contact the FTC
- on TV or radio, contact the FTC
- in person, call local police first



Investigator Joe  
Burdick

- Santa Clara County District  
Attorney's Office
- (408) 792-2330
- [jburdick@dao.sccgov.org](mailto:jburdick@dao.sccgov.org)

