WELCOME

SENIOR SCAM STOPPER SEMINAR
ASSEMBLYMEMBER ALEX LEE
24TH ASSEMBLY DISTRICT

PHONE: (408) 262-2501 | (916) 319-2024
EMAIL: ASSEMBLYMEMBER.LEE@ASSEMBLY.CA.GOV
WEBSITE: A24.ASMDC.ORG
PRESENTERS

DURRIYA SYED
California Department of Insurance

STEPHANIE GUTIERREZ-VALDEZ and MIGUEL GALARZA
California Contractors State License Board

KUE LEE
California Department of Financial Protection & Innovation

JOE BURDICK
Santa Clara County District Attorney’s Office
CALIFORNIA DEPARTMENT OF INSURANCE

Durriya Syed
Community Relations & Outreach Branch
How the Department of Insurance improves lives of Californians

- Protect consumers from fraud and abuse
- Regulate most lines of insurance and maintain insurer solvency
- Set standards for agents and broker licensing
- Perform market conduct reviews of insurance companies
- Resolve consumer complaints
- Investigate and prosecute insurance fraud
- Cannot require or compel insurance companies to sell insurance
Most Common Insurance Fraud

• Seniors are the largest population targeted for scams

• Why are seniors big targets?
Annuities

• What is it?

• Is it RIGHT for you?
  • Pros
  • Cons
Common Insurance Scams

- Premium Theft
- Staged Auto Accidents
- COVID-19 Insurance Fraud
Insurance Scam Warning Signs

• The agent
  • offers “free” seminars
  • offers “free” meals
  • offers to create or update a living trust
  • gives you wrong information about your current investments

• Senior Insurance Bill of Rights (SIBOR)
Avoid Becoming a Victim

- Check the status of insurance agent/insurance company
- Answer all questions thoroughly and truthfully
- Get everything in writing and compare policies
- **ASK QUESTIONS**
- Never feel pressured or intimidated
- Don’t sign anything you do not understand
Insurance Fraud Resources & Contacts

• Department of Insurance
  • 800-927-4357  www.insurance.ca.gov

• Senior Medicare Patrol
  • 855-613-7080

• AARP Fraud Watch Network Hotline
  • 877-908-3360

• Coalition Against Insurance Fraud
  • www.InsuranceFraud.org
Senior Resources from CDI

- Senior Gateway – [www.seniors.insurance.ca.gov](http://www.seniors.insurance.ca.gov)
- One-Stop Website – hosted by CDI
- Senior Information Guides

Follow QR Code:
Insurance Questions or Concerns

www.insurance.ca.gov

800-927-4357
What Seniors Should Know About Construction Scams
About CSLB

- Protects California consumers
- Licenses nearly 300,000 contractors in 44 different classifications

CSLB Headquarters, Sacramento, CA
Seniors are trusting, which can make them vulnerable

Unlicensed contractors will try to manipulate seniors

Scammers attracted to seniors' life savings and pensions
Do not answer your door to strangers selling their services

Just say no, and keep saying no

Do not make any cash payments
HOW TO AVOID COMMON CONSTRUCTION SCAMS

Get everything in writing; verbal agreements are not binding

Down payments can only be 10% or $1,000 of the contract price - whichever is less!

ALWAYS check the contractor license number to make sure it is current and in good standing at www.cslb.ca.gov or by calling 800-321-CSLB (2752)
IF YOU'VE BEEN SCAMMED

- Call CSLB: 1-800-321-CSLB (2752), or
- Visit www.cslb.ca.gov, "File a Complaint" on the homepage, or
- Email: cslbinfo@cslb.ca.gov
TIPS FOR HIRING THE RIGHT CONTRACTOR

• Get at least three bids
• Ask to see the contractor's pocket license and current photo ID
• Ask for proof of their liability insurance
• Make sure to get a detailed written contract before you make a down payment, and before work begins
• Don't let payments get ahead of the work. Don't pay for work that has not been completed to your satisfaction.
TIPS FOR HIRING THE RIGHT CONTRACTOR (CONTINUED)

- Pay no more than 10% of the total contract price, or $1,000 - whichever is less
- Keep all project documents, payments, photographs in a job file
- Seniors have 4 years from the date of construction to file a complaint
- Ages 65+ have a five-day right to cancel any contract (California law)
IS SOLAR RIGHT FOR YOU?

- Length of time in home
- Roof direction
- Do the math with solar
- Look at monthly statements

WWW.CSLB.CA.GOV/SOLARSMART
• Solar is not free
• Beware of financing programs: PACE, HERO, CHEEF, OR REEL
• High interest rates
• Tied to property taxes
PROTECT YOURSELF FROM SOLAR FRAUD

- Don’t let payments get ahead of the work
- Get everything in writing
- Make sure you understand the contract terms
ALWAYS CHECK A LICENSE & HIRE LICENSED CONTRACTORS FOR JOBS WORTH $500 OR MORE FOR LABOR & MATERIALS

VISIT WWW.CSLB.CA.GOV OR CALL 800-321-CSLB (2752) TO CHECK A LICENSE AND/OR FIND A LICENSED CONTRACTOR IN YOUR AREA
“The best ways seniors can protect themselves against construction fraud is to check a license on our website and always get at least three bids.”

- David R. Fogt, CSLB Registrar
Protect Yourself from Fraud and Scams

Kue Lee
Director of Targeted Outreach
Kue.Lee@dfpi.ca.gov
The Department of Financial Protection & Innovation

Who Are We? What Is Our Role?

- The DFPI is California’s licensing and regulatory agency of state-financial institutions, products, and professionals.

- We conduct exams to ensure compliance, review consumer complaints, and pursue legal actions against those operating illegally, or are using unlawful, deceptive, or abusive practices.

- We also provide financial education and consumer awareness presentations throughout California to inform and help protect consumers.

Learn more at: [https://dfpi.ca.gov](https://dfpi.ca.gov)
How is the DFPI Promoting Consumer Awareness?

- DFPI provides in-person and virtual presentations
- DFPI website features:
  - News and Consumer Alerts (www.dfpi.ca.gov/news)
  - Crypto Scam tracker (www.dfpi.ca.gov/crypto-scams)
  - Events and investor education (www.dfpi.ca.gov/events)
- FREE DFPI publications (www.dfpi.ca.gov/outreach)
- DFPI YouTube Channel (www.youtube.com/cadfpi)
The PACE Financing Program

What is PACE?

Property Assessed Clean Energy (PACE)

A program providing homeowners finance energy-efficient and water-saving improvements to their property.

[Insert website link]

www.DFPI.ca.gov/PACE
Use Caution with PACE and other Home-Improvement Financing Programs

Before signing the contract - be sure you check the license of both the contractor and the lender.

- To verify the Contractor, contact the Contractor’s State License Board at www.cslb.gov.

- To verify the Lender, go DFPI’s website at www.dfpi.ca.gov or call our Consumer Services Office 1-866-275-2677.

- For more information on the risks and laws, visit www.dfpi.ca.gov/PACE.
Romance Scams!!!!

In 2022 - 70,000 people reported a romance scam, and reported in the last 5 years losses hit a staggering $1.3 billion

- Average of $9,500 in losses each
Is Your Cyber Sweetheart Swindling You?

Roses are red, violets are blue, and romance scammers can fool you, too. Look for these red flags.

- They say they’re far away.
- Their profile seem too good to be true.
- The relationship is moving fast.
- They break promises to see you.
- They ask for money.
- They require specific payment methods.

Warning

STOP THINK PROCEED

DFPI DEPARTMENT OF FINANCIAL PROTECTION & INNOVATION
Common **Methods** Scammers Use to Contact You:

- **Vishing** - Telephone (home/cell)
- **Phishing** - Computer/Emails
- **Smishing** - Text Messages
  - “Click here”
  - “Callback number”

**DO NOT RESPOND**
to any of these attempts
to contact you!
HELLO...
WHO’S CALLING?

Trending Frauds & Scams

• Grandparent/Relative Scam
• Credit/Debit Card purchases
• Debt Collectors
• Government Imposters:
  ➢ IRS / Social Security
  ➢ Utility Company
  ➢ Financial Institutions

DO NOT RESPOND to any of these attempts to contact you!
Artificial Intelligence (AI) Scams

- [https://youtu.be/V6_jCGzR020](https://youtu.be/V6_jCGzR020)
- **FTC**: Scammers use AI to enhance their family emergency schemes ([https://tinyurl.com/dfpi322203](https://tinyurl.com/dfpi322203))
- **DFPI**: Launches Sweep of Investment Fraud Claiming Ties to Artificial Intelligence ([https://tinyurl.com/dfpi4192023](https://tinyurl.com/dfpi4192023))
EXAMPLE OF PHISHING

From: Bank of America <crvdqi@comcast.net>
Subject: Notification Irregular Activity
Date: September 23, 2014 3:44:42 PM PDT
To: Undisclosed recipients:
Reply-To: crvdqi@comcast.net

Dear member:

We detected unusual activity on your Bank of America debit card on 09/22/2014. For your protection, please verify this activity so you can continue making debit card transactions without interruption.

Please sign in to your account at https://www.bankofamerica.com to review and verify your account activity. After verifying your debit card transactions we will take the necessary steps to protect your account from fraud.

If you do not contact us, certain limitations may be placed on your debit card.

© 2014 Bank of America Corporation. All rights reserved.

http://bit.do/ghsdfhgsd

Online Banking Alert

Would be capitalized

Grammatical Error
EXAMPLE OF SMISHING

Text Message
Today 08:58
We have identified some unusual activity on your online banking. Please log in via http://bit.do/dq3WJ to secure your account.

Text Message
Today 1:43 PM
Notice-269078 from:Chase-Bank. Code: Your Card is temporary locked. Please call us now at 201-429-3304 to un-lock.

Text Message
Wednesday, 21 April 2021
DHL: Your parcel is arriving, track here: http://demo.mipunet.cn/a/?lrwlaqj8eo66
Money Apps / Transfer Scams

- Apps on mobile devices
- In-person storefronts
- Online

Free Msg-Suncoast Credit Union Alert-Did You Attempt a Zelle Payment for the Amount of $5000.00? Reply YES or NO or 1 to decline fraud alerts

NO
Website safety

Secure connection

https://www.securesites.com

Connection between your web browser and the website server is encrypted

Unsecured connection

http://www.unsecuredsite.com

Just like an ID card confirms a person's identity, a private key confirms server identity.

Missing “s”
Credit Reports: What You Need to Know

• Three major credit reporting agencies
• **Credit Bureaus must:**
  1. Make sure that the information they collect about you is accurate.
  2. Give you a free copy of your report once every 12 months (at your request).
  3. Provide you a chance to fix any mistakes.
• [www.annualcreditreport.com](http://www.annualcreditreport.com) or call 1-877-322-8228
• Other reasons for a free credit report:
  • Signs of identity theft
  • Freeze your credit
  • File a complaint
File a Complaint:

- CA Department of Financial Protection and Innovation (DFPI)
  - www.dfpi.ca.gov/file-a-complaint
- Federal Trade Commission (FTC)
  - www.reportfraud.ftc.gov
- Consumer Financial Protection Bureau (CFPB)
  - www.consumerfinance.gov/complaint
- CA Attorney General’s Office
  - https://oag.ca.gov/contact/consumer-complaint-against-business-or-company
- CA Department of Consumer Affairs (DCA)
  - www.dca.ca.gov/consumers/complaints/consumer.shtml
Be Careful with Crypto!

• **Currently crypto assets **ARE NOT **regulated.**

• Investing in or purchasing crypto assets **does not guarantee** that you’ll make money.
  • If someone is making that promise, it’s a big scam red flag.
  • Do your research! Gather information from more than one resource.

• Check government agency websites for scam information.

• Don’t rush into anything: Scammers prey on the fear of missing out (also known as “FOMO”).
Additional Crypto Assets Resources and Help

- DFPI Crypto Assets webpage:
  - www.dfpi.ca.gov/crypto

- DFPI Crypto Scam Tracker webpage:
  - www.dfpi.ca.gov/crypto-scams

- Securities and Exchange Commission's Crypto Assets and Cyber Enforcement Actions webpage:
  - www.sec.gov/spotlight/cybersecurity-enforcement-actions

- The Commodities and Futures Trading Commission’s Crypto assets webpage:
  - www.cftc.gov/digitalassets/index.htm

- The Federal Trade Commission’s Cryptocurrency Consumer advice webpage:
  - https://consumer.ftc.gov/search-terms/cryptocurrency
Safety Tips:
Protect Your Personal and Financial Information

- Don’t return phone calls to numbers left on your voice mail
- Unknown caller? Don’t answer or hang up.
- Never give your personal information unless you initiated the contact
- Government agencies DO NOT CALL you
- Do not click on unknown links
- Use a shredder for your mail and personal documents
- DO NOT drop off mail after pick up hours
- Use anti-theft gel pens for checks and other signature documents
- Don’t just close your Internet browser – be sure to log out of websites
- Limit information on social media!
Stay Connected to the DFPI!

• Subscribe to our newsletter: www.DFPI.ca.gov/subscribe

• Check out our other events: www.DFPI.ca.gov/events

• Call: (866) 275-2677
• Email: Ask.DFPI@dfpi.ca.gov
• Web: www.DFPI.ca.gov
• Social Media: www.DFPI.ca.gov/#social
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%.

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

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.
<table>
<thead>
<tr>
<th>TYPE OF ELDER FRAUD</th>
<th>NUMBER OF VICTIMS (2021)</th>
<th>TOTAL LOSSES (2021)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidence fraud/romance</td>
<td>7,658</td>
<td>$432,081,001</td>
</tr>
<tr>
<td>Business email/email account compromise</td>
<td>3,755</td>
<td>$355,805,098</td>
</tr>
<tr>
<td>Investment</td>
<td>2,104</td>
<td>$239,474,635</td>
</tr>
<tr>
<td>Tech support</td>
<td>13,900</td>
<td>$237,931,278</td>
</tr>
<tr>
<td>Personal data breach</td>
<td>6,189</td>
<td>$103,668,489</td>
</tr>
<tr>
<td>Real estate/rental</td>
<td>1,764</td>
<td>$102,071,631</td>
</tr>
<tr>
<td>Government impersonation</td>
<td>3,319</td>
<td>$69,186,358</td>
</tr>
<tr>
<td>Identity theft</td>
<td>8,002</td>
<td>$59,022,153</td>
</tr>
<tr>
<td>Lottery/sweepstakes/inheritance</td>
<td>2,607</td>
<td>$53,557,330</td>
</tr>
<tr>
<td>Non-payment/non-delivery</td>
<td>13,220</td>
<td>$52,023,580</td>
</tr>
<tr>
<td>Credit card fraud</td>
<td>3,164</td>
<td>$39,019,072</td>
</tr>
<tr>
<td>Advanced fee*</td>
<td>3,029</td>
<td>$35,464,491</td>
</tr>
</tbody>
</table>

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

Billing Department 5603990 angelijames7436@gmail.com to me

Hey jjuridick190
To determine when to renew, please refer to the attached file BillE81909131.

One attachment - Scanned by Gmail

Dear Customer,

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

Features: Norton 360 offers protection 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: 231.25 USD

In case there is anything unclear or if you have any questions, feel free to call us at 1-866-525-7745.

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

Thans & Regards
Norton
Business Imposters / Text Messages

Text Message
Today 11:40 AM

We have shipped your package LS908021, and charged your account for $1808. If you have any questions or need assistance, please contact us at +18445849493.

The sender is not in your contact list.
Report Junk

2:10

Text Message
Sun, Jan 22 at 10:30 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/mnexit-pc1032us

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

2:09

Text Message
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.cld/v6BzoiA

You can’t access your
“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

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 02-09-2014 | Priority: Urgent
Call center making fraudulent calls in Bangalore, India.
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

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!
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.
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.
All Fraud can always be reported to Adult Protective Services in your area. 1-800-414-2002
• through the mail, report to the USPIS
• on the internet, FTC at ReportFraud.ftc.gov
• 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
QUESTIONS & ANSWERS?
Thank you for joining us!

For more information, please contact us at

Assemblymember Alex Lee
Email: Assemblymember.Lee@asm.ca.gov
Phone: (408) 262-2501 | (916) 319-2024
Website: a24.asmdc.org