San Diego
Elder Justice Task Force

Scam Presentation
May 9, 2025

FBI Supervisory Special Agent Michael Rod

Oceanside PD Detective Sergeant Josh Young

WHAT IS ELDER FRAUD?

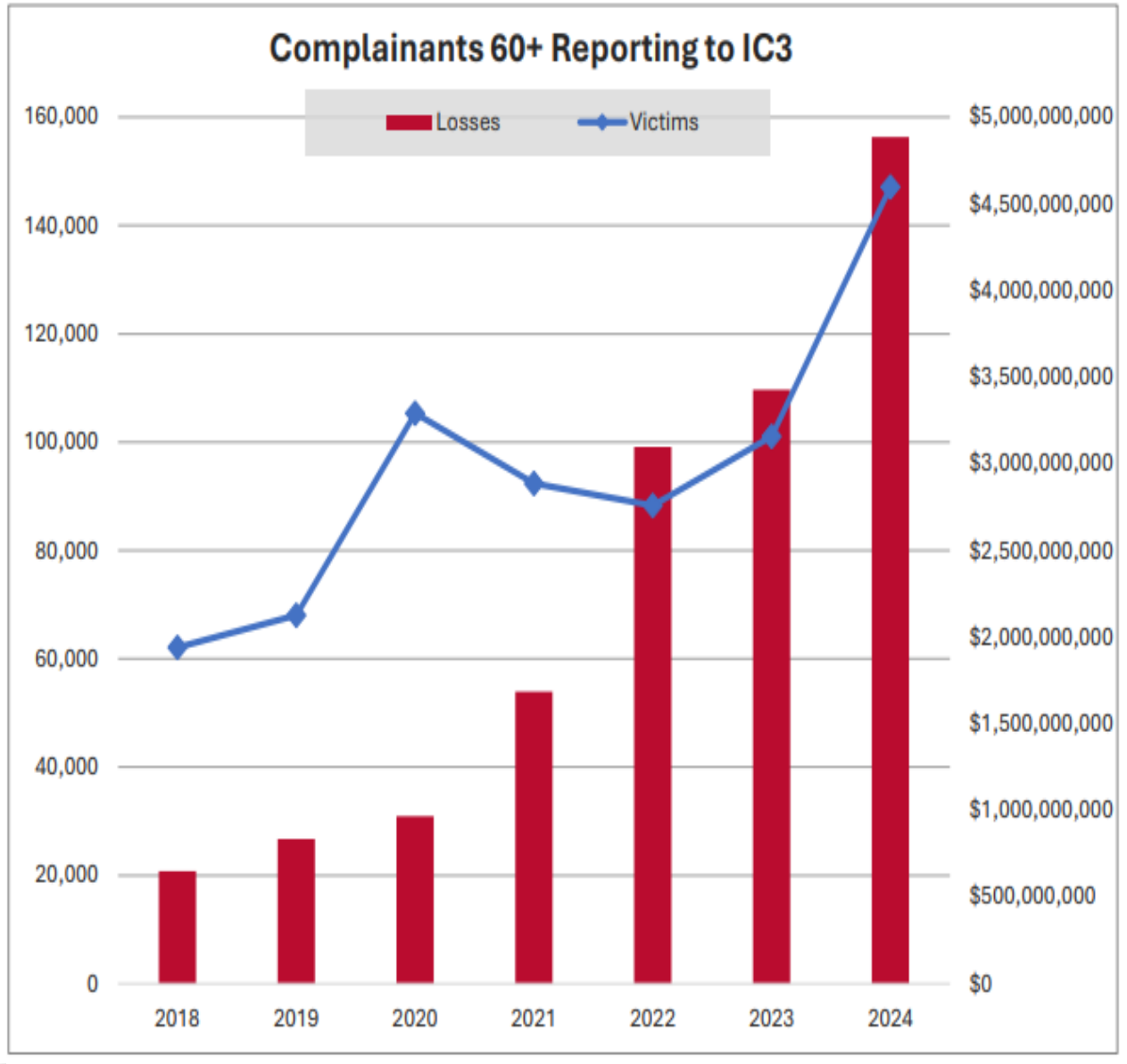
- **TRICKS AND SCAMS**
  - Limited only by the imagination of bad guy
  - Overseas actors
  - U.S. based facilitators / money mules
- **TARGETS (60+)**
  - Designed to target vulnerable population
  - Repeat victimization

Nationwide Stats

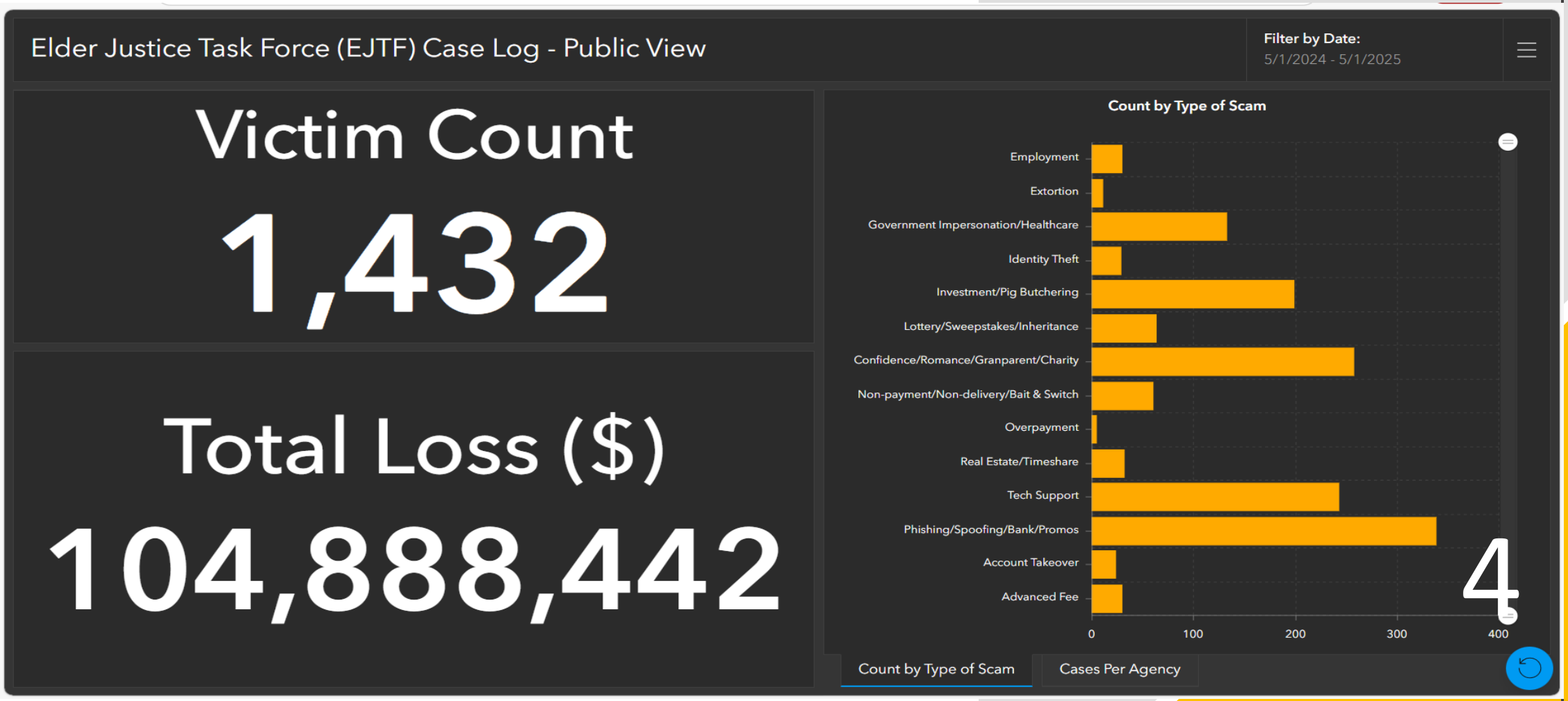
60+ COMPLAINTS - 2024

147,127 Complaints	$4.885 Billion in Losses	46% Increase in Complaints from 2023	43% Increase in Losses from 2023

7,500 Complainants Lost >$100K	$83,000 Average Loss



San Diego County Stats



OCEANSIDE STATS

2024

63 Online Financial Elder Scam Cases

Total Loss: 1.57 Million

2025 (Jan – April)

21 Online Financial Elder Scam Cases

Total Loss: $500,000

Tech Support

How it works

1. Pop-up Message from Tech Support
2. Call the phone number on the pop-up
3. Call from Tech Support Team
   - Transferred to Bank, Refund Specialist or Government Imposter

What you can do

1. Don’t call the phone number
2. Don’t click any links
3. Do not provide access to your computer
4. **Slow down**
5. **Phone a friend**

Case Example 1

- 70 year-old victim attempts to log into Charles Schwab account.
- Pop-up appears telling victim their account was hacked, and to call a phone number.
- Victim calls the number and speaks to scammer, who claims that a corrupt Wells Fargo employee perpetrated the hack.
- Scammer convinces victim they must withdraw all cash from their account for their own protection.

Case Example 1

- Scammer directed victim to withdraw $50,000 cash to be picked up by a “Wells Fargo Representative”.
- When courier arrived at victim’s home, the victim became suspicious and took a photo of them.
- After the pickup, suspect directed victim to retrieve another $40,000 cash.
- Wells Fargo became suspicious and rejected the victims attempts.
- Victim contacted OPD, who assisted in luring a second courier back to the residence.

Case Example 1

- Victim contacted OPD, who worked with the victim to arrange a second pickup by the suspects.
- When the next courier arrived on the victim’s street, he refused to exit his vehicle to make the pickup.
- After driving up and down the victim’s street several times while trying to get the victim to come to his vehicle, courier was stopped by Detectives and arrested.

Case Example 1

- After 30 days in custody, courier plead guilty to felony financial elder abuse.
- As part of his plea agreement, courier agreed to pay the victim $30,000.
- The check had to be successfully cashed prior to his release.
- Courier was placed on probation with his 4th amendment rights revoked for 2 years.

Case Example 2

- *Victim received email RE: test results from MyScripps.com.*
- *While attempting to open results, a full-screen "pop-up" appeared, advising her computer was hacked and to call Microsoft Tech Support.*
- Upon calling the number, victim was transferred to several other scammers, who claimed her SDCCU bank accounts were compromised.

Case Example 2

- Scammers directed victim to make cash withdrawals to “help protect her money from hackers.”
- Scammers directed the victim to several SDCCU branches to withdraw a total of $25,000 cash from her account.
- Scammers remained in contact with the victim throughout the process, directing her to tell the bank she “needed the cash to buy property from an old friend.”
- The following day, scammers sent a courier to pickup the cash from the victim at her home.

Case Example 2

- Scammers then convinced the victim to liquidate the rest of her savings and exchange it for gold bars, which they would send an additional courier to pick up.

- The gold vendor who the victim went to caught onto the scam and contacted EJTF, who notified Oceanside PD.

Case Example 2

- EJTF and OPD conducted surveillance at the victim's residence, ultimately intercepting the next courier coming to do the pickup.
- The suspect, who was expecting to pickup $360,000 in gold bars, was arrested and booked for Financial Elder Abuse, Attempted Grand Theft and Conspiracy.
- Suspect remains in custody, awaiting trial on a $1,000,000 bond.

Domino Effect: It’s not just financial loss

- Loss of perceived relationship in romance scams
- Loss of assets
- Loss of trust in self and others
- Risk of re-victimization
- Loss of support system
- **Impact on mental health**

Reminders

- Don’t send money to someone you don’t know.
- Don’t respond to messages that ask for personal or financial information
- Don’t agree to deposit a check from someone you don’t know.
- Read your bills and monthly statements regularly.
- Remember there is no such thing as a sure thing.
- Know where any offer comes from and who you’re dealing with.

Immediate Action Items

- **Contact your bank and report the fraud.**
- **File a police report and IC3 complaint – www.ic3.gov**
- **Contact the three major credit bureaus:**
- Experian (1-888-397-3742), TransUnion (1-800-680-7289) & Equifax (1-800-525-6285) and
- Place a “Fraud Alert” on your credit report.
- Close all tampered or fraudulent accounts.
- Follow up in writing with copies of supporting documents
- Obtain copies from any/all police reports (you will likely need to forward these reports to relevant parties).

Internet Crime Complaint Center (IC3)

File A Complaint | Public Info | Industry Info | Cyber Private Sector | Crime Info

Welcome to the Internet Crime Complaint Center

The Internet Crime Complaint Center (IC3) is the central hub for reporting cyber-enabled crime. It is run by the FBI, the lead federal agency for investigating crime.

For more information about the IC3 and its mission, please see the About Us page.

File a Complaint with Us

If you or someone else is in immediate danger, please call 911 or your local police.

The IC3 focuses on collecting cyber-enabled crime. Crimes against children should be filed with the National Center for Missing and Exploited Children. Other types of crimes, such as threats of terrorism, should be reported at tips.fbi.gov.

File A Complaint

Resources

- National Elder Fraud Hotline: 833-FRAUD-11 (833-372-8311)
- Identity Theft Resource Center: 888-400-5530
- AARP Fraud Watch Network Helpline: 877-908-3360
- FTC Consumer Alerts at www.ftc.gov
- IRS Taxpayer Advocate: www.taxpayeradvocate.irs.gov
- Peer Support Program for Romance Scam Survivors: www.fightcybercrime.org
- Public Service Announcements - www.IC3 .gov

Best Solution: Prevention!

Be wise to the scams!

Don’t let them win!

Lean on your friends!

- ✓ Neighbors
- ✓ Family
- ✓ OPD (760-435-4911)

Thank You

REMEMBER:

- Slow Down
- Phone a Friend
- Call OPD (760-435-4911)