2025 CEFLI ANNUAL CONFERENCE

FRAUD

What Are the Fraudsters Up to Now?

HOTEL DEL CORONADO | SAN DIEGO, CALIFORNIA | SEPTEMBER 14-16, 2025

Speakers

Vickie Bulger

Senior Vice President, Insurance Chief Compliance Officer

Primerica Life

Kathie Weber (Moderator)

Shareholder

Maynard Nexsen

Dayna Kendall

Special Agent

FBI

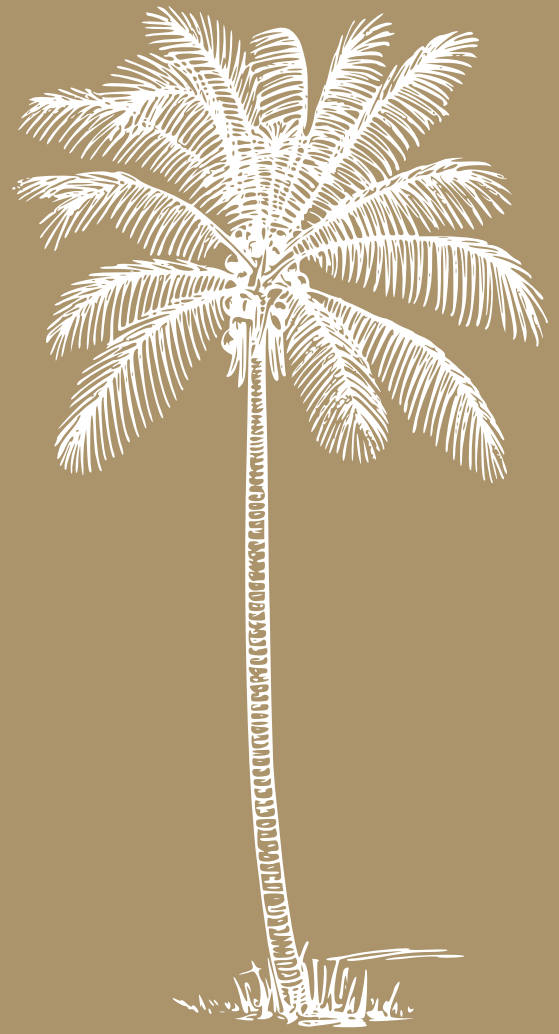
Carlota Balet Gusils

Financial Crimes Officer

Allianz Life

Agenda

- Panel Introductions
- Fraud Defined
- Fraud By The Numbers
- What are we still seeing, how are things changing, and what's new?
- Questions
- Resources



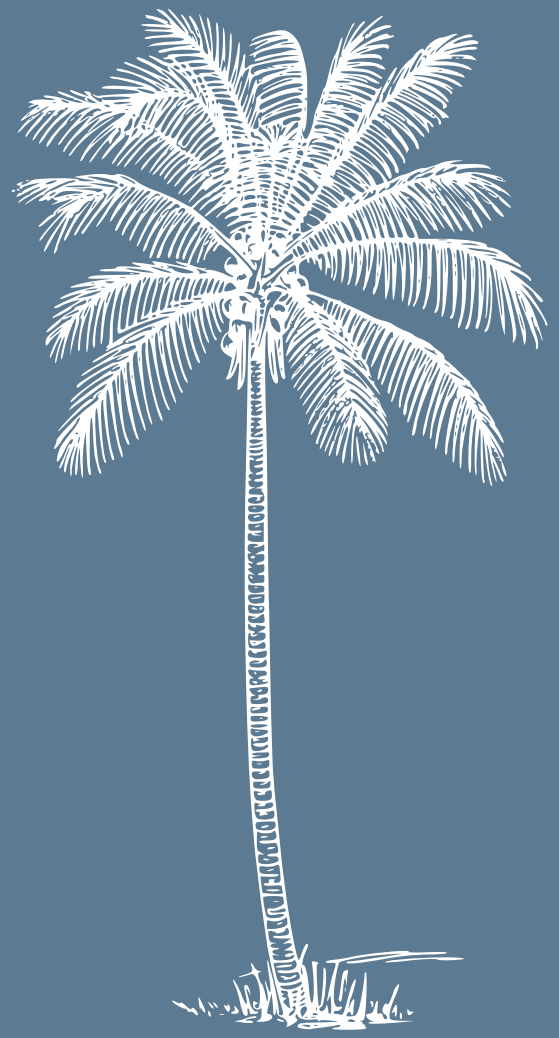
Fraud Defined

Fraud Defined

As noted, in part, in NAIC Model Regulation 680 (Insurance Fraud Prevention Model Act), a **fraudulent insurance act** is an act or omission committed by a person who, *knowingly and with intent to defraud*, commits, or conceals any material information concerning one or more of the following: an insurance application, rating of an insurance policy, claim payment, or premium payment etc.

The definition of *insurance fraud* may vary by state. For example, in California: fraud occurs when someone knowingly lies to obtain a benefit or advantage to which they are not otherwise entitled, or someone knowingly denies a benefit that is due and to which someone is entitled.

Fraud By The Numbers

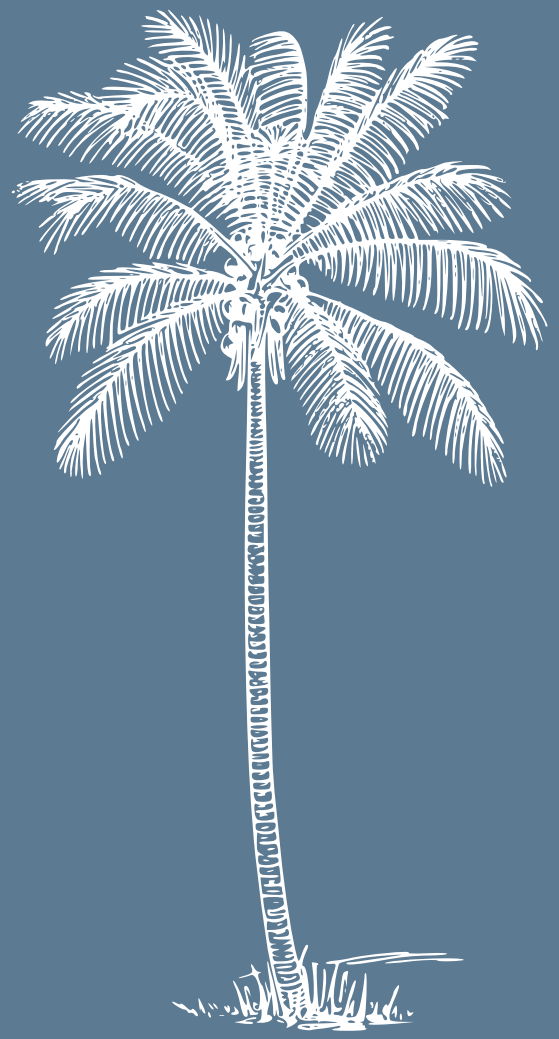


Fraud By The Numbers

$308.6B- the annual cost of insurance fraud to U.S. consumers and businesses

Life Insurance constitutes approximately **$74.7B** of that according to the Coalition Against Insurance Fraud and Colorado State University Global

www.Insurancefraud.org (Coalition Against Insurance Fraud)



Fraud By The Numbers

SAR filings as of 08/28/25 for 2025 | 5,247 filings in the life/annuity space

- ACH- 1,710
- Advance Fee- 2
- Check- 149
- Consumer Loan- 33
- Credit/Debit Card- 8
- Excessive Insurance- 6
- Excessive or Unusual Cash Borrowing against Policy/Annuity- 100
- Healthcare/Public or Private Health Insurance- 7
- Mail- 19
- Mass Marketing- 2
- Other Fraud- 1,567
- Other Insurance- 85
- Ponzi Scheme- 1
- Proceeds Sent to or Received from Unrelated Third Party- 14
- Securities- 1
- Suspicious Life Settlement Sales Insurance (e.g., STOLI, Viaticals)- 4
- Suspicious Termination of Policy or Contract- 55
- Unclear or No Insurable Interest- 17
- Wire- 1,467

https://www.fincen.gov/reports/sar-stats

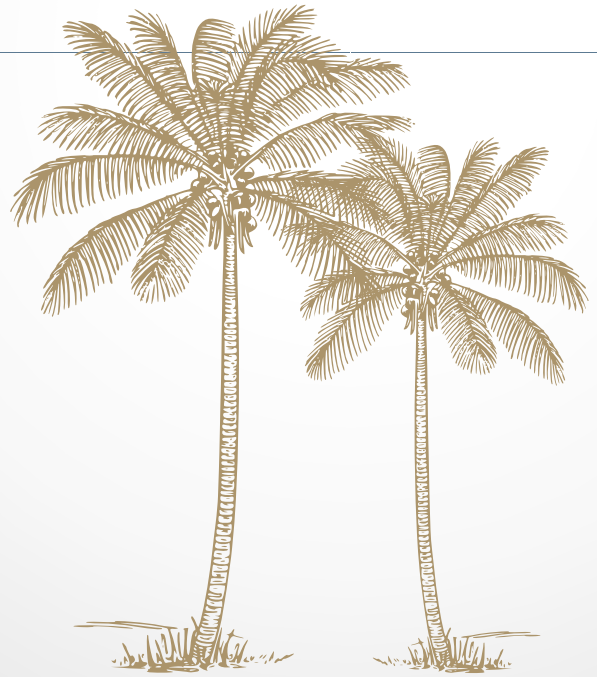
Now

What are we still seeing, how are things changing, and what's new?

What are we still seeing, how are things changing, and what's new?

- Account Takeover (ATO)
- AI & Synthetic ID Fraud
- Elder Financial Exploitation
- Stranger-Owned Life Insurance (STOLI)
- Agent-Involved Fraud Schemes
- Email Compromise Fraud
- Internal Fraud
- HR/Employment Fraud

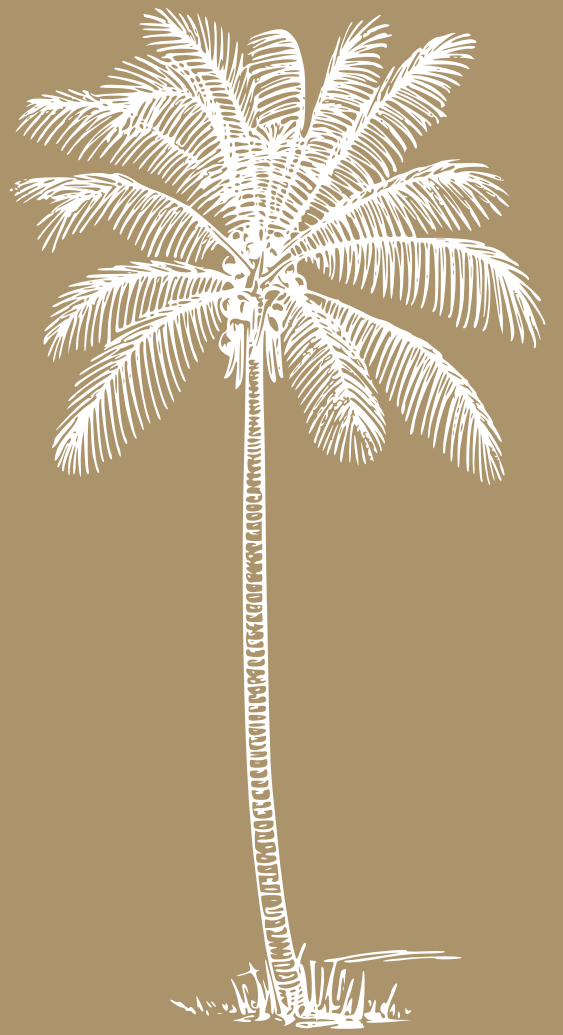
Account Takeover (ATO)

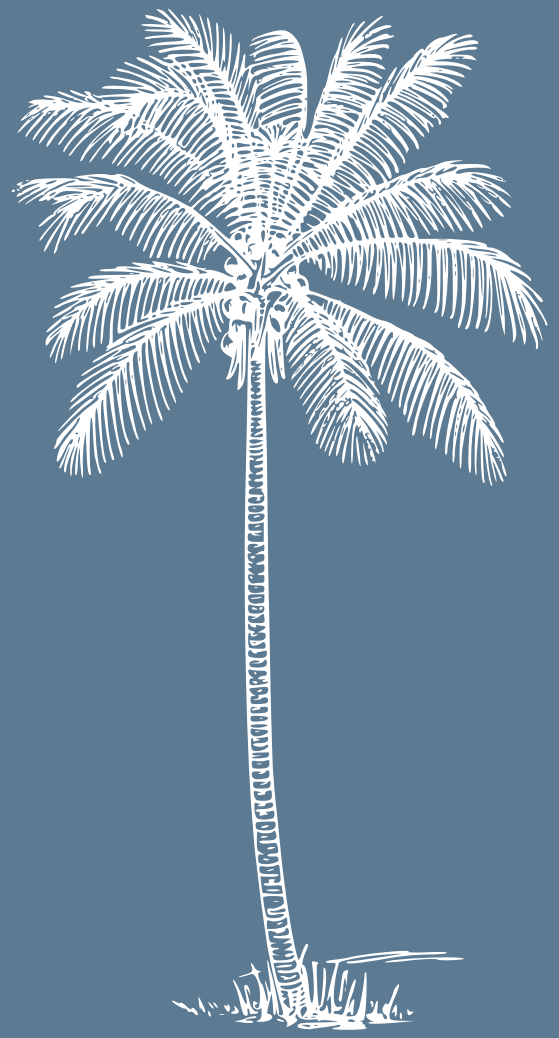


- Still happening- likely due to the number of data breaches that have occurred
- Data is "out there", and insurance carriers and financial services typically collect the same data
- AI contributes to consumer impersonation
- Still ATO with a technology spin
- Banking environments with questionable validity still being used & bank KYC
- Speed of access is increasing - phone number masking is very common

Internal ATO

- Historically, when we think account takeover, we think it originates externally
- Internal case- The individual had a work laptop, and – the hypothesis was there's either somebody sitting next to them or they had a personal device next to them - where they were capturing information and then going in and modifying data from an external lens and impersonating the customer.
- *How do you prevent your customer service individuals from accessing certain data that would potentially prevent that or how do you become aware of it?*





AI & Synthetic ID Fraud

AI- Fraudsters utilizing AI to gain access to accounts and to emulate the consumer voice

Synthetic Identity Fraud- occurs when criminals combine real and fictitious information to create a new identity, and the new identity is used to open accounts or submit false claims. The synthetic identify is comprised of real data, social security numbers and fake information, which makes it more difficult to identify.

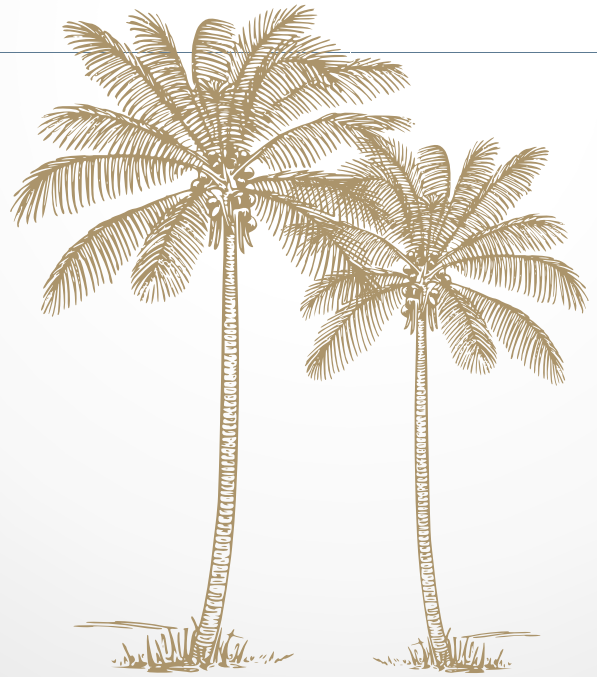
Elder Financial Exploitation

- ✓ Focus is on identifying a victim
- ✓ Spending time developing trust
- ✓ Sprinkling fake drama all over the place to set the stage
- ✓ Victim unknowingly/knowingly cashes out policies and hands over the proceeds

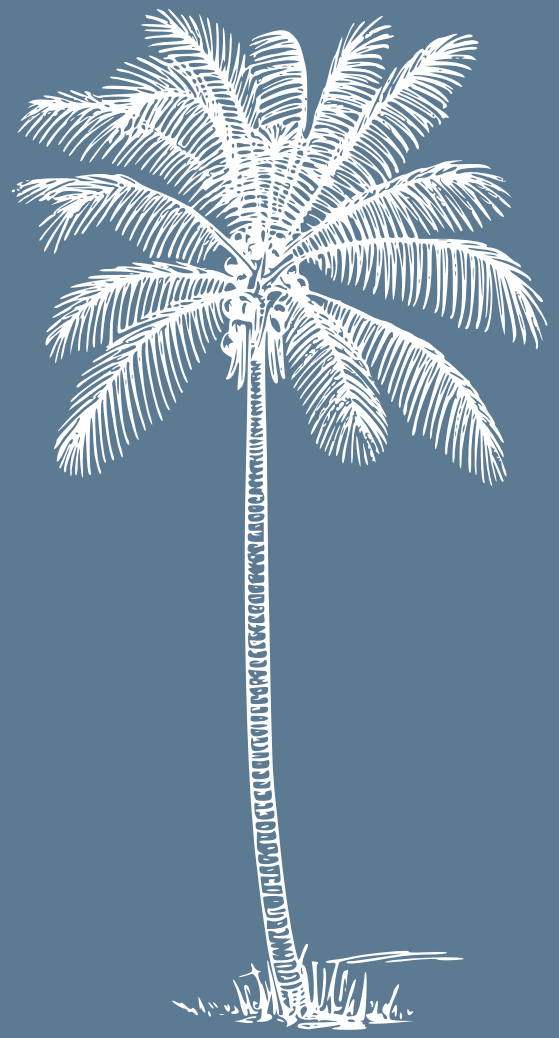
Who can help these victims?

Adult Protective Services Law Enforcement The FBI

Stranger-Owned Life Insurance (STOLI)



- What is STOLI?
- Recent STOLI cases
- Not as prevalent as it once was, but it's still happening
- Seeing some agent-based activity with tenuous familial relationships noted on applications



Agent-Involved Fraud Schemes

Advanced Commissions Schemes

- simplified issue (auto) applications
- agents submitted multiple in a very short time
- alerted in one case by the Postal Inspector - advised that he had a tub full of mail that went to a vacant address, all different names on it, all life policies

Combatting

- review of bank account numbers
- new things related to persistency
- Monitor for a large uptick in policy activity. Stop the commission payments until it can be further investigated.
- Identifying multiple policies drafting from one bank account.
- Agent writing application without applicant's knowledge and/or with questionable information on the application.
- Agent submitting an application or changes to coverage or beneficiary *following* an insured's death.

Email Compromise Fraud

Victims click on a targeted ad via an attachment or link, and malware is installed on the computer

- Targeted ads appear in social media or email servers

Malware allows bad actors access to everything

- Conduct transactions
- Personal information
- Update settings, to include updating settings, stopping alerts and auto-deleting emails and notifications

Often the first time victims learn anything is wrong is when they check their bank account and money is missing

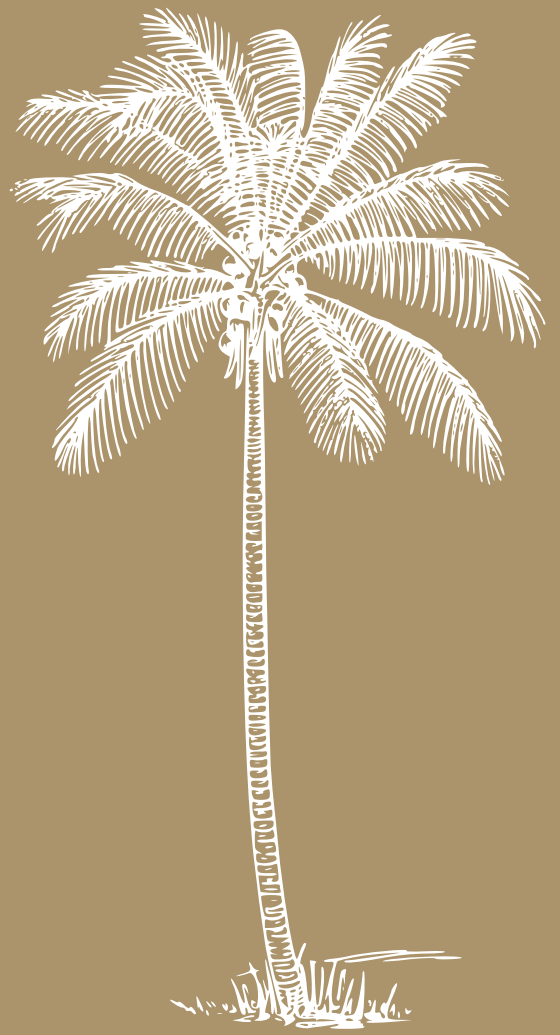
Internal Fraud

Fake Documents

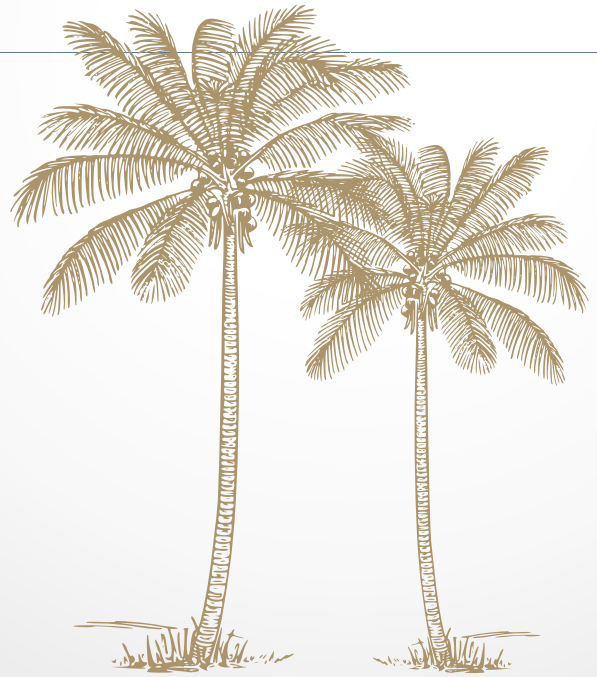
Bad actions create false insurance company policy documents or vendor information

Social Engineering

Fraudsters pretend to be Tech Support or another known external vendor and convince employee to provide them with system access or security information so that they can access company systems



HR/ Employment Fraud



- Is the employee really who they claim to be?
- How are they verified?
- What's in the news…
- Remote workers be required to appear in person at least once or periodically

Questions?

Resources

These are linked on CEFLI.org

Resources > Additional Resources > Fraud Resources

Resources

Department of Justice

- National Elder Fraud Hotline 1-833-FRAUD-11 (833) 372-8311

Florida Department of Financial Services

- Fraud and Scams - Your Guide to Outsmarting Scammers
- Insurance Fraud Guide (PDF)

FBI Fraud Resource Page Common Frauds and Scams

North American Securities Administration Association Fraud Center Page Fraud Center

AARP Scams & Fraud Scam, Fraud Alerts - Protect Your Digital Identity

FINRA

- Senior Investors
- Three Resources for Senior Investors
- Protecting Yourself from Fraud: Navigating an Evolving Landscape
- Protect Your Money [*Check Registration: Sellers and Investments; Avoid Fraud; Safeguard Your Identity; Watch for Red Flags*]

Up Next

Networking Lunch 12:15 – 1:15 PM (*Southpointe Lawn*)
Sponsored by **The Berwyn Group**

Breakout 1 1:15 - 2:00 PM COMPLIANCE TECHNOLOGY: AI Use Cases for Compliance (*Southpointe East & West*)

– OR –

Breakout 2 1:15 - 2:00 PM COMPLIANCE STRATEGIES: Market Conduct Exam Management and Trends (*Southpointe A-D*)