# FRAUD ON THE RISE

**Real Stories, Real Strategies, Real Solutions**

# AGENDA

MOST COMMON FINANCIAL CRIMES

AI AND EMERGING TRENDS

EFFECTIVELY COLLABORATING WITH LAW ENFORCEMENT

FINAL TIPS & TAKEAWAYS

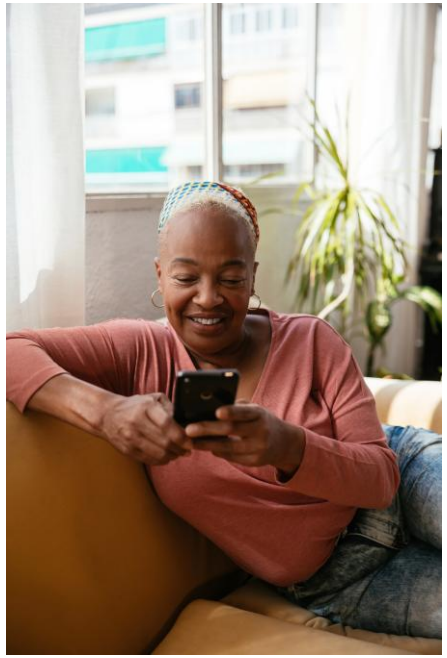
# MOST COMMON FINANCIAL CRIMES

- Investment Scams/Crypto
- Phone/Text Impersonations
- Grandparent and Imposter Scams
- Tech Support Scams
- Mass Mail Scams
- Romance/Relationship Scams
- Counterfeit Check Scams
- Compromised Email Accounts


# CURRENT ELDER FRAUD TRENDS

- Bank accounts being opened online using victim PII
- Victims opening bank accounts and providing their debit cards and PINs to fraudsters who conduct ATM withdrawals
- Increasing reports of in person currency or gold pickups from victims
- Fraudsters using retailers as parcel pickup locations instead of their home address (Walgreens, grocery stores)

# WHY IT'S WORKING



Everyone is on social media and/or a cell phone

Real-time payments remove the float through platforms like Zelle, Venmo, and CashPay

Caller prompts them to buy gift cards or go to a crypto ATM outside of the banker's view

The caller tells client to lie if asked why they are transferring or withdrawing so much money

Caller claims to be a government official or other authority

Limit on how much banks can do to prevent the transaction, absent closing the account

# WHAT IS CAUSING INCREASE IN FRAUD?

- Unprecedented levels of mail theft causing surge in check fraud
- Increasing use of APP and Fintech
  - FBI's IC3 received more than 149,686 fraud complaints of cyber-enabled crime and fraud involving cryptocurrency, with over **$9.3 billion in reported losses**
- Transnational Scam Centers
- Multi-tiered scams involving bank or law enforcement impersonations
- Scams that target bank employees

# CURRENT TRENDS

## ARTIFICIAL INTELLIGENCE ON THE RISE

# DEEPFAKES IN FRAUD SCHEMES

**Synthetic Media Creation**

Deepfakes use artificial intelligence to create highly realistic videos or audio, simulating things never actually said or done.

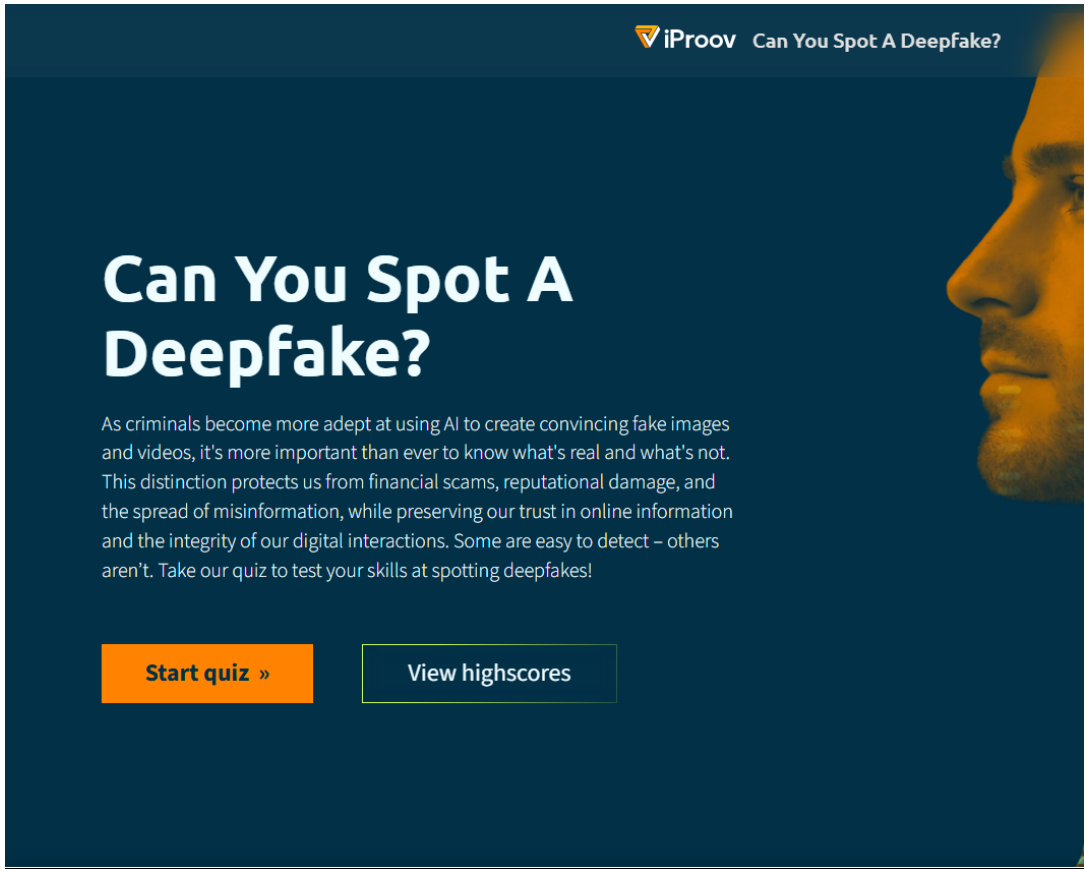
**Fraudulent Uses of Deepfakes**

Criminals leverage deepfakes to fake voices or manipulate videos for scams and unauthorized transactions.

**Authentication and Security Risks**

Deepfake techniques present major challenges for verifying identity and maintaining digital security.

# ARTIFICIAL INTELLIGENCE IS INCREASING LEGITIMACY




- AI used to write scripts/emails/letters
- Auto-dialers
- Analytics
- Spending less time on the fraud – casting a wider net, scraping social media
- Deep Fakes - disguise voices, accents, and their video

https://quiz.iproov.com/

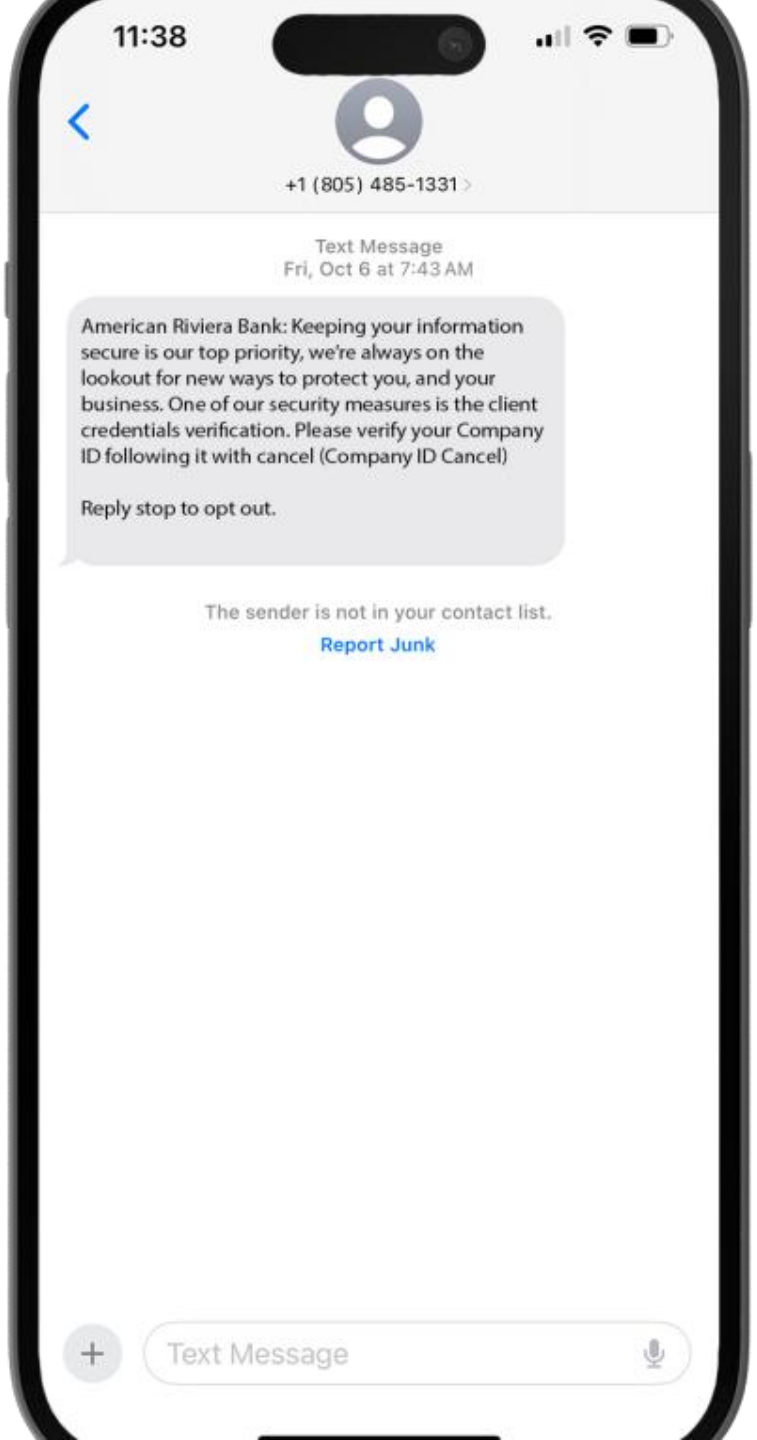
# HOW VOICE WORKS IN A DEEPFAKE

Only need 6 seconds of your voice

- Pitch variation
- Tone & cadence
- Accents
- Phrases

Researching location and online presence for queues enhances the message, making it more impactful and believable

- Restaurants
- Activities
- Interests on social media




# BANK IMPERSONATIONS

New trend away from suspicious debit card transactions to credential theft

- Consider brand protection services for identifying look-alike domains and assisting with takedown
- Ensure proper investigation under Regulation E; consumers are not liable if someone unauthorized uses stolen credentials
- Beware—businesses are not covered by Regulation E, but you may still be subject to litigation costs

## Virtual Assistant Opportunity

LOGO

Dear Students and Alumni,

We are currently offering a remote Virtual Assistant position for students interested i

**Details:**

Weekly Stipend: $350

Time Commitment: ~7 hours/week (flexible)

Duration: 6 weeks

**Responsibilities include:**

Organizing digital materials

Assisting with scheduling and email communication

Supporting administrative tasks and light data entry

**Eligibility:**

Applicants must be currently enrolled or previously enrolled in a university program.

**To Apply:**

Email Professor First Last at (firstlast50@gmail.com) with:

Full Name

Contact Number

Alternate Email

Academic Department

Year of Study

Positions are limited, so early applications are encouraged.

Best regards,

Professor First Last

Santa Cruz, CA

# OVERPAYMENT SCAMS USING STOLEN CHECK DATA

Students see a job posting on college campus board for a Virtual Remote Assistant job

Apply for this position and are “hired” and sent a counterfeit check that appears to be drawn off the University

Instructed to Zelle $$$ back to a sales representative who “worked” for the same company

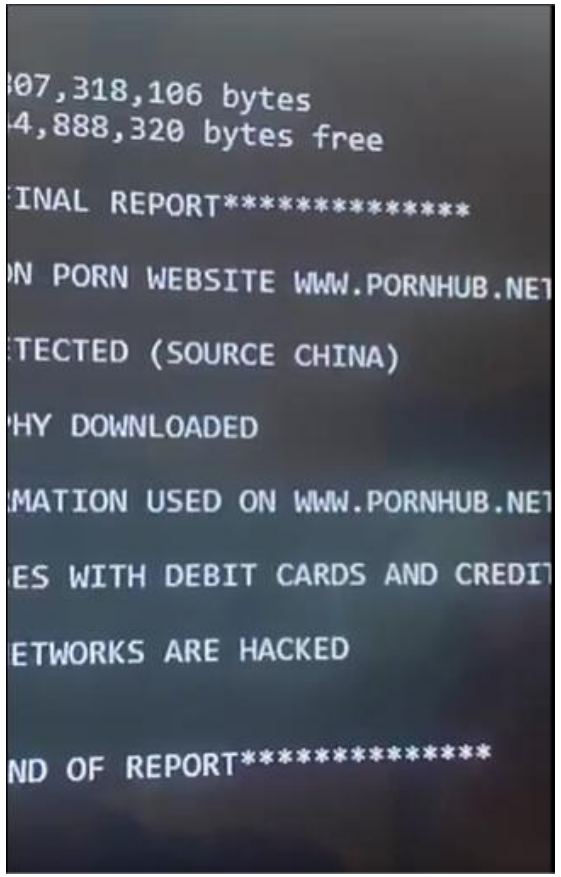
# TECH SUPPORT CRIMES

Fraudster calls and pretends to be a computer technician from a reputable company saying their computer has been infected.

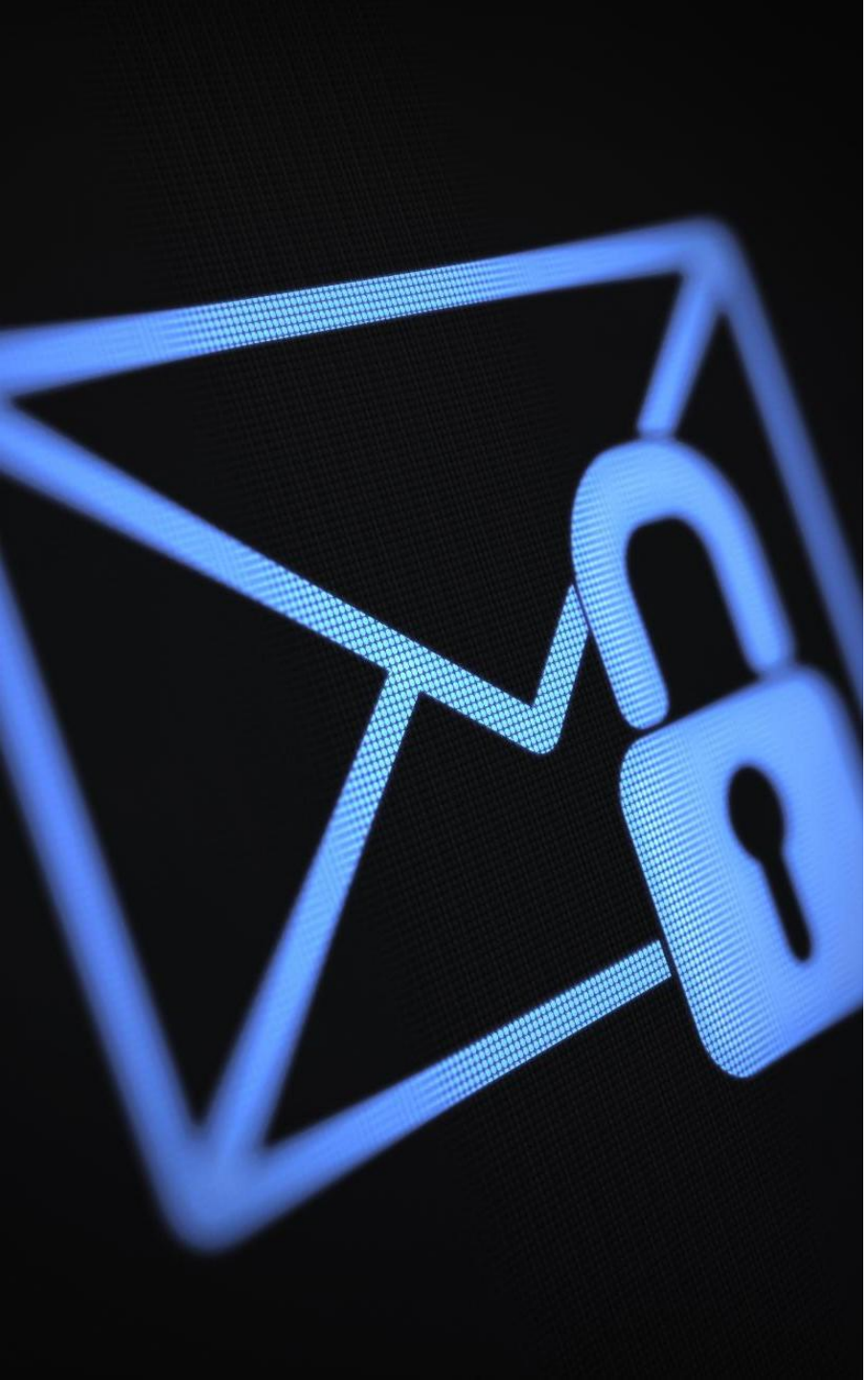
A popup window says your computer is at risk. The message in the window warns of a security issue on the computer and to call a number to get help.

1. Fraudulent ‘Refund’ where fraudster tells victims they are owed a refund for prior services, requiring a credit card, or
2. Ransomware- fraudster installs malware that holds your computer ‘hostage’ demanding money for access.

Guidance for victims: *https://www.consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams*




https://www.youtube.com/watch?v=IHINL7047E0



# SPOTTING LOTTERY SCAMS

**Scam Claims**

Scammers impersonate Publishers Clearing House, or other lotteries, falsely telling victims they have won prizes to trick them.

**Requests for Money or Information**

Fraudsters may ask for payments or personal information. Assure victims that legitimate prizes never require payment.

**Protective Actions**

Instruct clients to verify all messages, avoid clicking suspicious links, and report scams to authorities to stay safe.

# CONVINCING VICTIMS

## TRAUMA-INFORMED STRATEGIES

# EMERGING BEST PRACTICES FOR UNDOING INTENSE UNDUE INFLUENCE

**Plant seeds of doubt: Quietly help the victim to realize the nature of the scam**

Small hypocrisies and inconsistencies lead to doubt (as opposed to direct attack on core beliefs)

By listening to the victim, you are more likely to find those inconsistencies

**What to say/do**

Use non-defensive questions (Wow, great that you won a prize. How do they determine that? Where do they get the money?)

"Here is what I think is happening. Can you describe the details of what is going on?"

Have the victim voluntarily tell the story of what happened and quietly raise hypocrisies

Make a list of Promises Made/Promises Kept by the con and by the victim

Ask for something the criminal cannot provide (such as a request for a live video chat for a celebrity impostor fraud) – make sure the criminal can't provide it

**Reflective listening/person-centered approach (Rogerian therapy)**

Explore what is happening, including discrepancies in the claims

Focus on one incident of a failed promise to raise hypocrisies

Focus on values as a means of self-affirmation

Explore the possibilities of positive alternatives—friends, family, groups

# OTHER STRATEGIES

We've reviewed your recent transactions as part of an ongoing fraud investigation, which indicate that you may be engaged in activity that violates state and/or federal criminal laws. The fraudulent activity may include the sending and/or receiving of funds (currency, checks, and/or money orders), gift cards, and/or wires related to a fraud scheme.

Perpetrators of these fraud schemes mislead victims into believing they are in a romantic relationship and deceive them into sending them money. Your continued involvement could be taken into consideration by law enforcement if you continue to be involved in this type of activity.

- ☐ Have you been asked by a stranger, friend, or family member to wire funds out of your account for any reason?
- ☐ Have you received a call from a friend or family member who needs money wired immediately and provided you with instructions for answering questions about the purpose, such as "it's a private matter"?
- ☐ Has anyone befriended you, online or in person, and is now asking you to wire money?
- ☐ Has anyone purporting to be law enforcement, or the government (Internal Revenue Service) contacted you via phone or email stating that you owe money and threatening legal action if you don't wire the funds?

The undersigned, _____ ("Customer"), has made a request to wire funds from their account with Bank. Customer hereby acknowledges that they have been advised by Mandated Reporter that this request exhibits certain red flags for financial fraud as described above. Customer also acknowledges that Mandated Reporter has advised them not to send the wire transfer, but Customer chooses to proceed. Customer accepts all risks of loss and agrees to hold harmless the Bank, its employees, agents, directors, and shareholders, for all losses, claims or demands on account of this wire transfer request.

If you wish to send this wire, please contact me at the number below.

1. Consider developing an escalation process
2. Use of templates in-branch may also help
3. Contact law enforcement and/or APS to pay a visit to the victim

# PARTNERING WITH LAW ENFORCEMENT

- Develop lists from existing cases
- Setup meetings
- Invite speakers
- Join multidisciplinary teams, including https://theknoble.com/
- Obtain as much information as possible when reports are filed
- Encourage victims to report, even if no or small loss amount

# REPORT FRAUD TO LOCAL POLICE/ APS & FEDERAL GOVERNMENT AGENCIES

- www.ic3.gov FBI Internet Crime Complaint Center
- www.reportfraud.ftc.gov Federal Trade Commission
- www.identitytheft.gov Report Identity Theft to the FTC
- https://www.uspis.gov/report U.S Postal Inspection Service or report by phone 1-877-876-2455

If Crypto Investment Confidence Fraud/Crypto-Romance Investment - contact your local U.S. Secret Service office, in addition to filing an IC3 report.
https://www.secretservice.gov/contact/field-offices

# TAKEAWAYS/TIPS

## Fraud playbook and/or victim guides

- Leverage Industry Victim Guides (The Knoble, FINRA) to develop your own escalation process to interact with victims
- Playbook for frontline to ensure sufficient details for working with law enforcement

## Resource lists for victims

- FightCyberCrime.org https://fightcybercrime.org/programs/romance-scam-recovery-group/
- AARP Fraud Watch Hotline-1-877-908-3360 and 1-888-687-2277
- National Elder Fraud Hotline-1-833-FRAUD-11 or 1-833-372-831

## Law enforcement

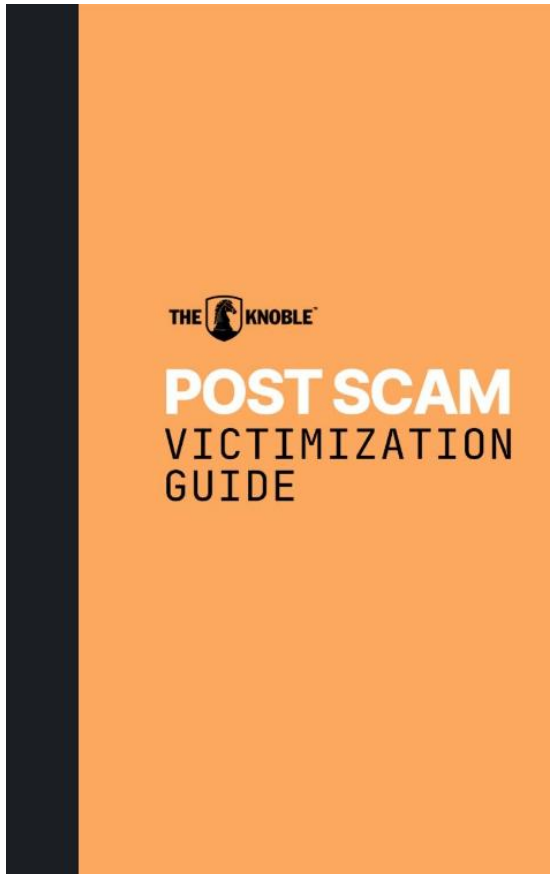
- Develop contact lists

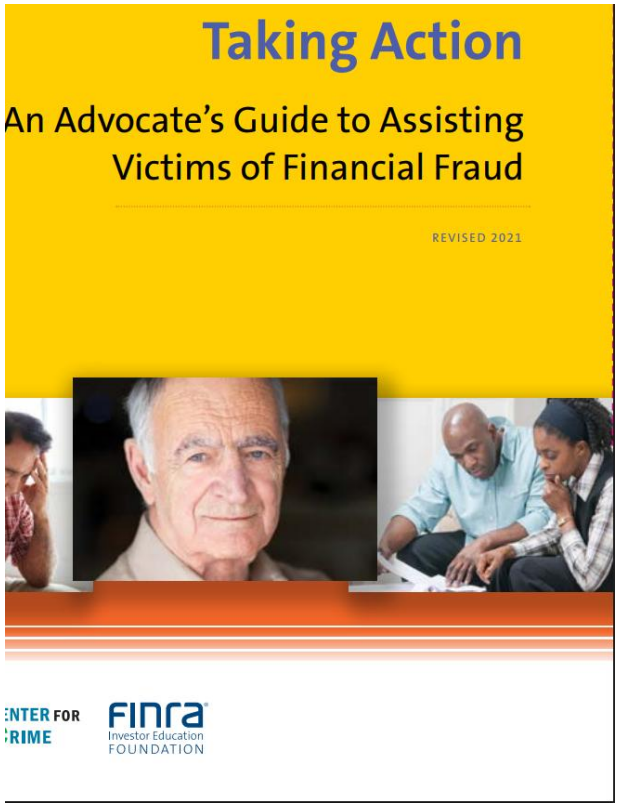
## Training

- BankSafe is a free resource
- Interactive training
- Develop resource list to stay current on evolving trends, such as artificial Intelligence

## Conduct a fraud risk assessment and investigate solutions

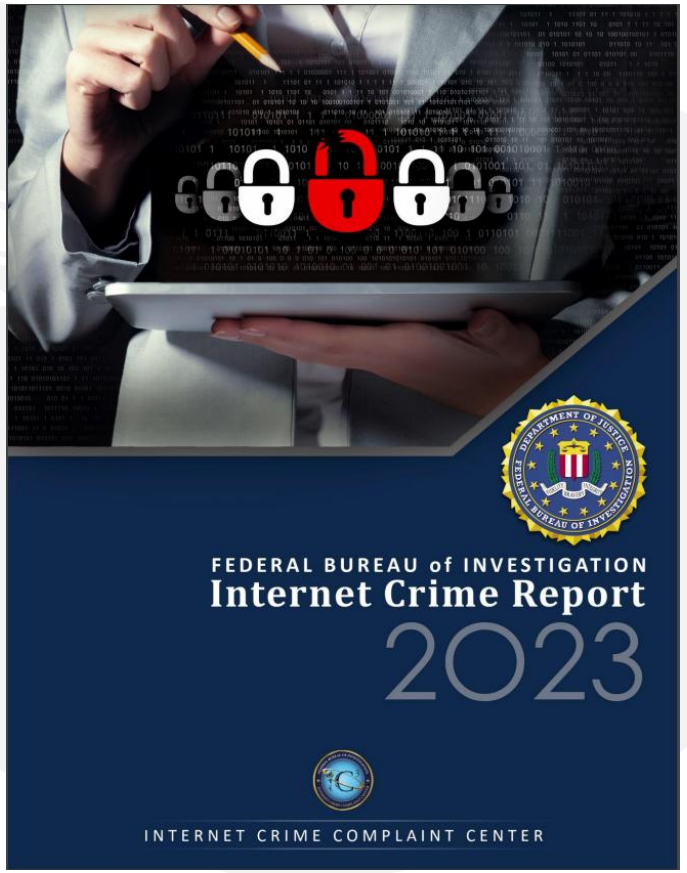
- Fraud monitoring
- New account controls



# TIPS TO RECOVER FUNDS

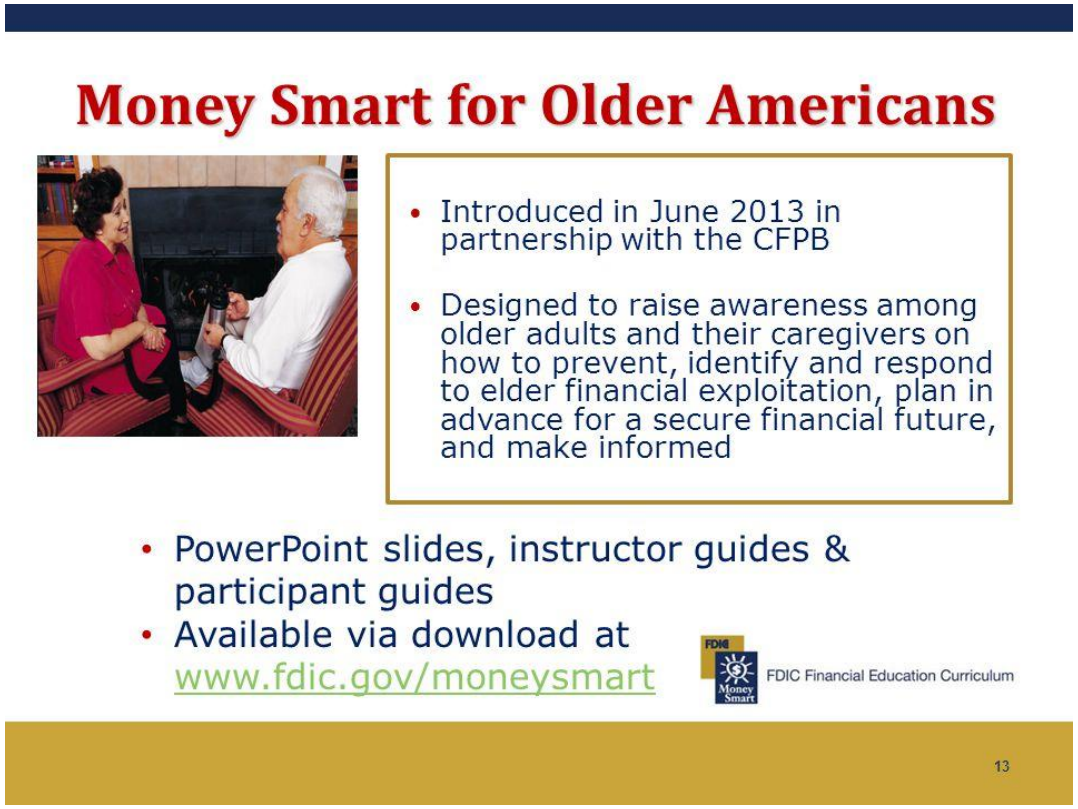
- File the SAR
  - Include all financial transaction information and any information on the fraudster
  - Save all correspondence, money transmission receipts, whether by text, emails, etc.
  - Download a copy of the victim's complaint when filed - victims cannot access a report once it is submitted.
- FBI Rapid Asset Recovery Team (RAT) works to block certain fraudulent wire transfers in BEC crimes by contacting financial institutions quickly to freeze suspicious pending wire transfers and return funds to victims.
- SUA's allow for 314B sharing on SARs with other financial institutions who have opted in



# FRONT-LINE MATERIALS

| | |
|---|---|
| **What is the check for?** | If it appears suspicious (loan to pay medical debt, investment opportunity, a "friend")<br><br>Ask: how did you receive it?<br><br>• If mail, report to USPIS and contact our local reps to determine whether the address is a known fraud address.<br><br>Notify the client a hold will be placed. If they appear upset or "need to send money now", that should be a red flag. Zelle funds typically cannot be recalled after they are sent. Consider contacting digital.<br><br>• You can offer to call to verify the check and release the hold |
| **What is the purpose of the cash withdrawal?** | If suspicious and drawn on uncollected funds probe further.<br>Ask: Where are you taking the cash?<br><br>· If Bitcoin ATM, report to the Secret Service.<br>· If cash was mailed, report to USPIS.<br>· If cash was used to buy gift cards, contact the company to determine if they have been redeemed. |
| **Do you need access to this deposit immediately?** | If yes, ask:<br>• Who are you sending the money to?<br><br>• How did you meet the person who gave you the check/asked you to send a wire/Zelle/buy the gift cards?<br><br>• Did they warn you not to tell the bank or say "it's a private matter"?<br><br>• If yes, "This sounds like a scam. Let me send you some information to review before you speak to them again." |
| **Did you give out any personal information?** | If yes<br>1. Flag the account as Identity Theft and file a QAR with the details of the case.<br>2. Have the client visit the IDtheft.gov checklist.<br>3. Ask them whether they clicked on any links or allowed access to their computer. |
| **Did they tell to go to a link or download anything?** | If yes, these may contain malware or phishing attempts.<br><br>If you did click or scan them, did you enter any of your personal details or download any apps from third-party sources (i.e., anywhere other than the official Google Play store or Apple app store). |
| **Did the person threaten legal action or to freeze your account?** | If yes, ask if they have contact information for the person who contacted them. |

# OTHER SOURCES FOR EXTERNAL TRAINING MATERIALS




- BankSafe through NAPSA
- CFPB / FDIC Money Smart
- ABA Foundation Safe Banking for Seniors
- FTC Pass-it-On
- https://operationshamrock.org/

# STAY CURRENT ON EVOLUTION OF SCAMS

Pig Butchering

Romance Scam (10 minutes)

https://www.youtube.com/watch?v=vthPmLORVrM

https://consumer.ftc.gov/articles/what-know-about-romance-scams

Tech support scams in practice

https://www.youtube.com/watch?v=wHpFNiTaup0

https://www.youtube.com/watch?v=OXngHr3VgUY

Grandparent Scam (7 minutes)

https://www.c-span.org/video/?c5093648/philadelphia-attorney-tells-lawmakers-fell-victim-ai-scam

CRYPTO / TECH / POLICY

**A bank exec stole $47 million for a crypto scam, and now he's going to jail**

/ Former Heartland Tri-State Bank CEO Shan Hanes was sentenced to 24 years in prison after getting caught up in a 'pig butchering' scam.

By Emma Roth, a news writer who covers the streaming wars, consumer tech, crypto, social media, and much more. Previously, she was a writer and editor at MUO.

Aug 23, 2024, 9:08 AM PDT

8 Comments (8 New)

Image: Cath Virginia / The Verge; Getty Images

# TECHNOLOGY SOLUTIONS TO COMBAT THE PROBLEM

- Client solutions
- Report fraud online
- Identity verification
- Positive pay for checks and ACH
- Real-time transaction monitoring
- Fraud detection solution
- Artificial Intelligence / Machine Learning

AI/Machine Learning

- Recognizing patterns using AI algorithms
- Providing real-time detection
- Reducing false positives
- Incorporating automation
- Integrating with other data sources
- Using natural language processing (NLP)
- Reducing costs

Don’t forget training for your staff /clients

# ABA-ENDORSED SOLUTIONS

| | | | |
|---|---|---|---|
| **Abrigo** | Abrigo Fraud Detection | AI-powered check fraud detection (currently in-clearing expanding to deposit) | Risk Platform |
| **Advanced Fraud Solutions** | TrueChecks | Real-time deposit fraud detection via consortium that includes access to EWS | Consortium |
| **ARGO** | OASIS and SAND | Comprehensive check fraud detection (deposit and in-clearing) | Point Solution |
| **Dark Defend, A Threat Advice Company** | TA Fraud Sentry | AI-powered fraud detection with dark web monitoring | Point Solution |
| **DataVisor** | DataVisor Check Fraud Solution | End-to-end AI-powered fraud detection | Risk Platform |
| **Featurespace** | ARIC Risk Hub | Enterprise financial crime prevention platform with check fraud capabilities | Risk Platform |
| **FIS** | DirectLink Risk Review | Integrated check fraud detection | Core banking processor |
| **Fiserv** | Multiple solutions, including ARGO, OASIS, TrueChecks, EWS | Suite of check fraud detection solutions | Core banking processors |
| **Infosys** | Infosys | AI-powered check fraud solution | Point Solution |
| **Mitek** | Check Fraud Defender | AI and computer vision-based fraud detection | Image analysis and forensics platform |
| **Nasdaq Verifin** | Check Fraud Detection and Mitigation | Consortium-based fraud detection | Risk Platform |

# THANK YOU

Christine Reins-Jarin, U.S. Postal Inspector
U.S. Postal Inspection Service, Transnational Elder Fraud Strike Force
CAReinsJarin@uspis.gov

Laurel Sykes, EVP
Chief Risk Officer
American Riviera Bank
lsykes@arb.bank