



# The Future of Fraud

2024

# PRESENTERS



**LAUREL SYKES**

Laurel Sykes is EVP and Chief Risk Officer for California-based American Riviera Bank, with offices in the Santa Barbara and San Luis Obispo Counties



**TODD ROVAK**

Todd Rovak is the Co-Founder and CEO of Carefull, a financial protection platform for older customers and their next generation families



# Agenda

- Increasing Losses will Significantly Impact Bank Profitability
- How Victims are Solicited and Why it Works
- Most Common Financial Crimes
- Solutions
  - Ensure Regulatory Compliance
  - Technology
  - Education and Awareness
  - Reporting for Recovery of Funds



# Banks are Being Hit from All Channels


- It is estimated more than **\$36 billion is stolen from older adults every year** by scammers and other types of theft
- Mail theft is facilitating a **surge in check fraud**
- APP Fraud
  - According to an Alloy survey of over 400 FI's, nearly 60% of banks, fintechs, and credit unions lost over **\$500K in direct fraud losses in 2023**
  - 22% of Alloy respondents ranked **APP fraud** as their top fraud type by case volume
  - Experian reports **APP fraud represents 41%** of all attacks



# Elder Fraud: California is taking legislative action

- SB-278 is the newest law to protect older Californians from **elder fraud and exploitation**, requiring:
  - Financial institutions to establish an emergency financial contact program
  - 3 day hold on suspicious transactions
  - Must be in place by Jan 2026





# What is Causing Increased Bank Losses?

- SB 278 and Reg E liability
- Chip present shifts liability to the bank
- Unprecedented levels of mail theft causing surge in check fraud
- Increasing use of APP and Fintech
  - FBI's IC3 received more than 69,000 complaints of cyber-enabled crime and fraud involving cryptocurrency, with over **\$5.6 billion in reported losses**
- Multi-tiered scams involving bank or LE impersonations

# Victims are Solicited through Text, Phone, Email or Social Media

Hello.  
My name is Ms Isabella Reece from Adecco Staffing Agency, USA. Are you looking for job opportunities? We are currently in need of staff. Kindly is it okay to briefly share the details?

Coinbase: Recovery and verify your wallet within 24 hours at <https://atruersound.com/coin> to avoid loss of balance.

U.S.Customs: You have a USPS parcel being cleared, due to the detection of an invalid zip code address, the parcel can not be cleared, the parcel is temporarily detained, please confirm the zip code address information in the link within 24 hours.  
<https://usbelived.xyz/YnMndsgVAt>

(Please reply with a Y, then exit the text message and open it again to activate the link, or copy the link into your Safari browser and open it)  
Have a great day from the USPS team!

Anna, I heard there is a new coffee shop in Chinatown, let's try it together

Are you busy?

Hello mom this is tenley can you bring me my sleeve I think they are on the table

Please I forgot them

I tried messaging you on the messaging application but you're not responding. Check it please

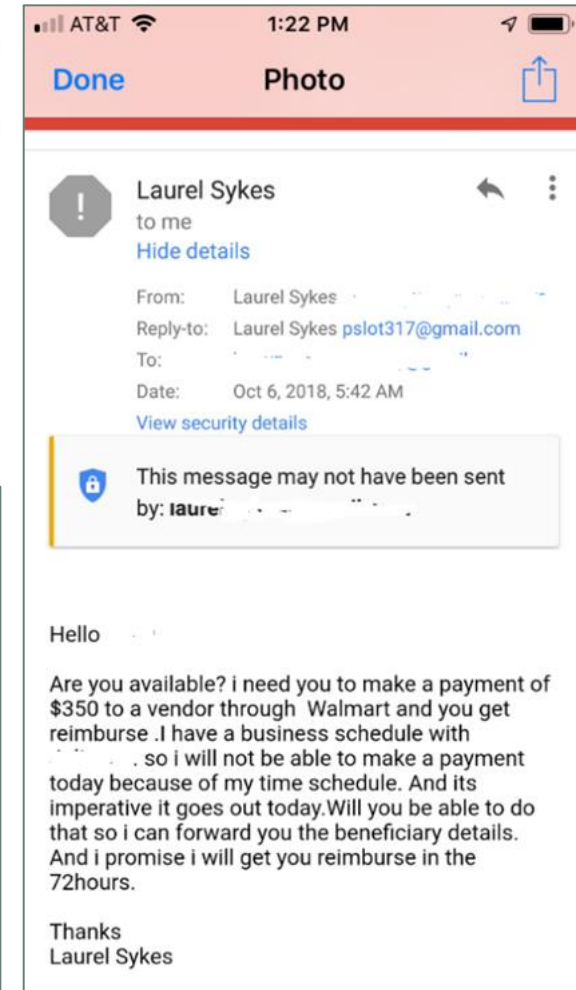
## Administrative And Operating Expenses

Today at 9:39 AM

Hi Laurel,

I will need you to take care of a payment to a vendor for me via EFT or Wire Payment, confirm if you can get it done today and i will provide you with the Vendor's beneficiary details you need in making the payment.

Regards



# Why it works

- 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 cryptocurrency ATM that are **outside of the banker's view**
- The **caller tells client to lie** to anyone who asks why they are transferring or withdrawing so much money
- Caller claims to be a **government official** or other authority

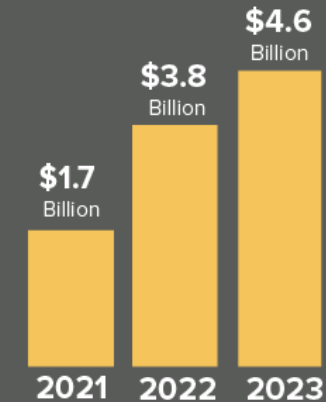
## IMPOSTER SCAMS

2023 By-the-Numbers Snapshot



According to the FTC, the imposter scam was the most common type of scam in 2023.

(Based on reports: [ftc.gov/data](https://www.ftc.gov/data))



**Phone Calls:**  
Highest per person reported losses. \$1,480 median in losses.



**Social Media:**  
Highest overall reported losses. \$1.4 Billion total in losses.



**Email:**  
Highest number of reports. 358,000 reports in 2023.





HAPPENING NOW

New York City commemorates 23rd anniversary of September 11 attacks. Watch live

World / Asia

# Finance worker pays out \$25 million after video call with deepfake ‘chief financial officer’



By Heather Chen and [Kathleen Magramo](#), CNN

2 minute read · Published 2:31 AM EST, Sun February 4, 2024



- Rapid rise in Gen AI use to enact fraud with deepfakes content through **emails, voice, and video**
  - Enables DIY fraudsters to execute more sophisticated social engineering scams
  - Voice recording can generate an imitation “deepfake” version that can be used to gain access to insurance or financial institutions



# Most Common Financial Crimes

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



**Scam Alert**  
⚠

**Voice Phishing (Vishing) Alert**

You receive a call from someone posing as a bank representative asking for sensitive and private account information. Another option is they want to send you a password authentication code.

Once they are in your account, they use the P2P system to transfer money out of your account. Draining your funds!

**Remember:**  
*Your bank will never ask for this information!*

 AMERICAN RIVIERA BANK  
*Bank on better.*

# 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=wHpFNiTaupQ>

<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



Image: Cath Virginia / The Verge; Getty Images

/ 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 MITO.

Aug 23, 2024, 9:05 AM PDT

[Share](#) [Facebook](#) [Twitter](#) [Comments \(8 New\)](#)

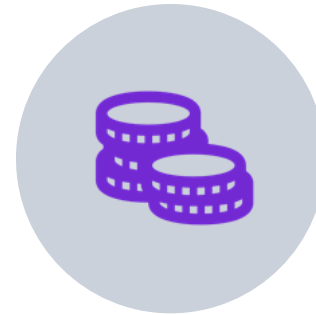
# Investment Scams / Pig Butchering



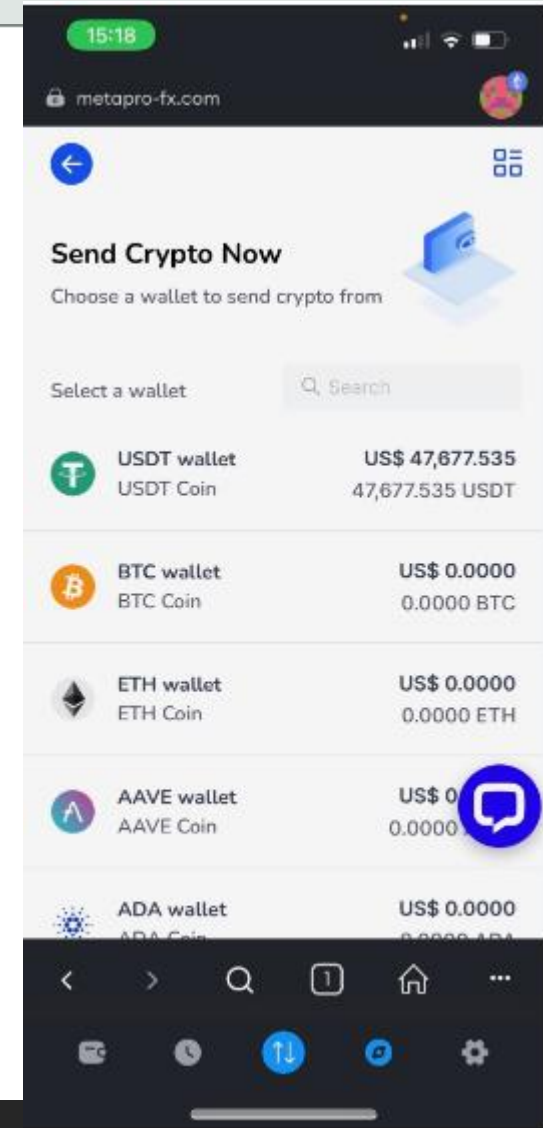
CONNECT WITH  
SOMEONE ONLINE OR BY  
TEXT



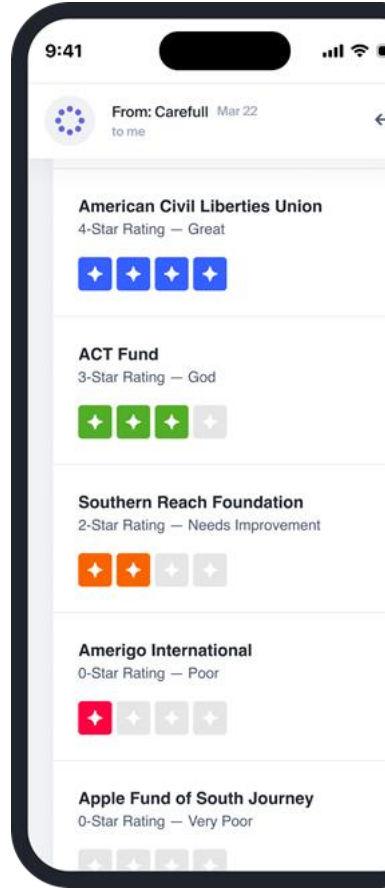
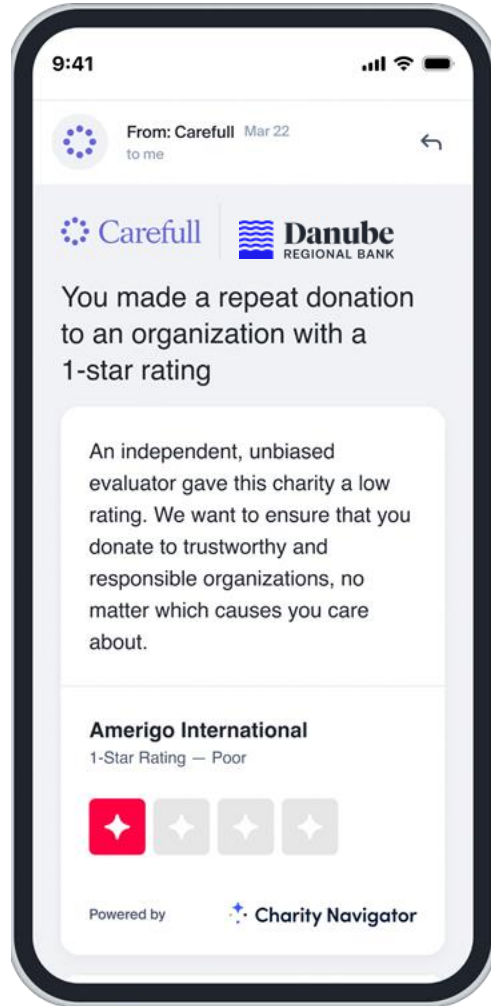
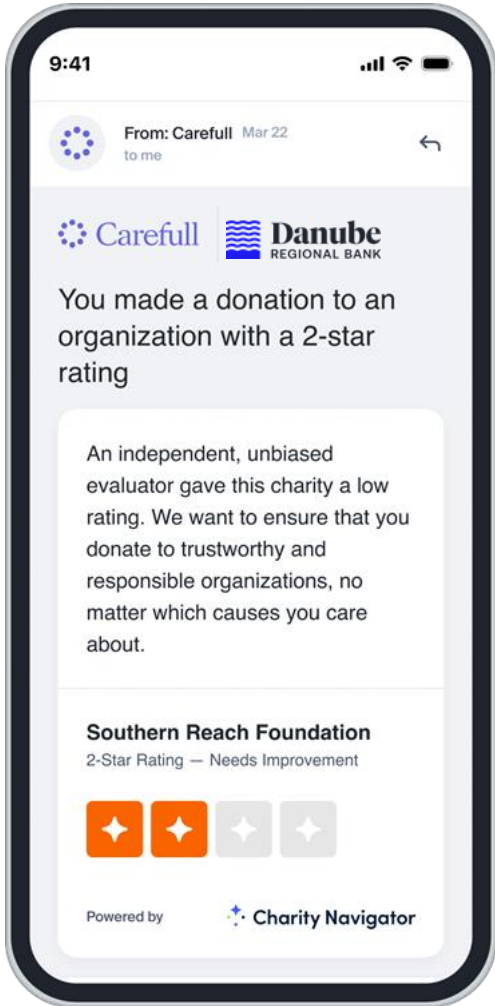
THEY ASK YOU TO INVEST



THEY SHOW YOU  
“PROFITS”



# Charitable Donation Scams



# Amazon Impersonations

---

- Request that client purchase a gift card for any service
- Ask you to download or install any software to connect with customer service to receive a refund
- Ask you to pay for something over the phone

Transaction Update: Your account is being debited for iPhone 13 USD \$599.97. Not you? Call Amazon at (888)\*\*\*-\*\*\*\*

## Anatomy of an Imposter Scam

Did you get a call about suspicious activity in your Amazon account?

**It's a scam. Hang up.**



# Amazon Impersonations

- Request that client purchase a gift card for any service
- Ask you to download or install any software to connect with customer service to receive a refund
- Ask you to pay for something over the phone

Potential Gift Card Purchase Close ×

Carefull's systems have detected that your may have purchased a gift card.


Date	Merchant	Amount
08/10/2024	Walgreens	\$ \$100.00


Account	Category
Synovus - Personal Checking *2...	Shops, Pharm...

[Get Help](#)

Was this alert useful?

**Related Articles**

 **Watch Out for Gift Card Scams** [Read](#)

 **How to Avoid Gift Card Scams** [Read](#)

## Hack Recovery

We'll lock out hackers, limit and reverse any damage caused, then set up protections to keep hackers out in the future.

[Begin](#)

## The steps we'll cover

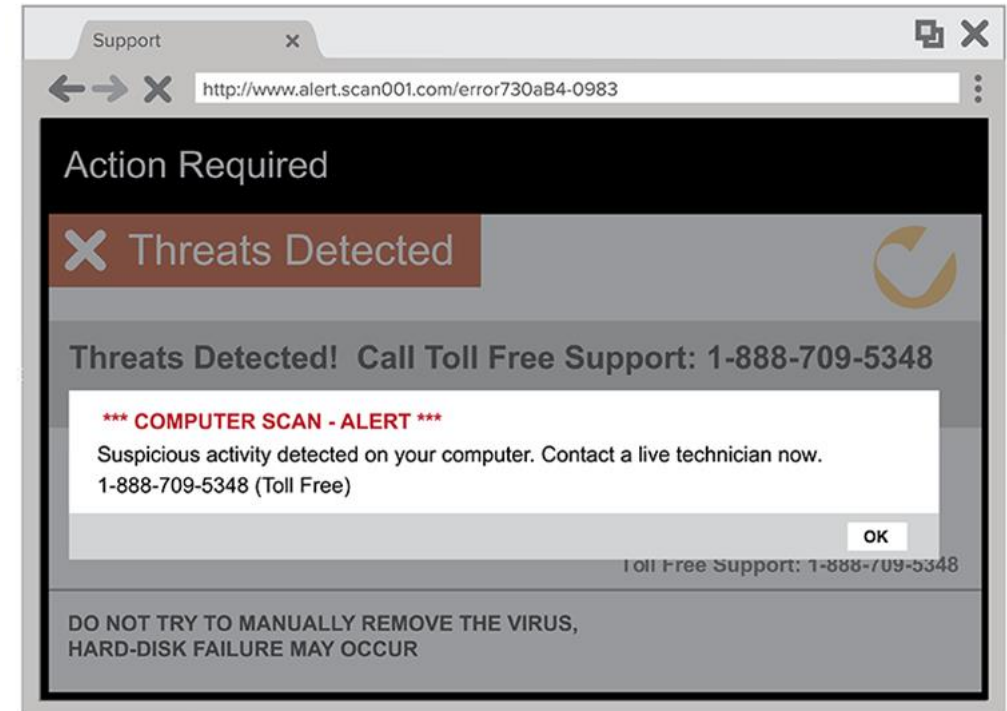
We'll walk you through all the necessary steps. Moving quickly is important to help limit the damage.

[Continue](#) →

- 1 Secure your devices
  - 2 Secure your email accounts
  - 3 Secure your financial accounts
  - 4 Freeze your credit
  - 5 Secure all your online accounts
  - 6 Review your transactions and messages
- [We save your place if you close Hack Recovery or need to step away.](#)

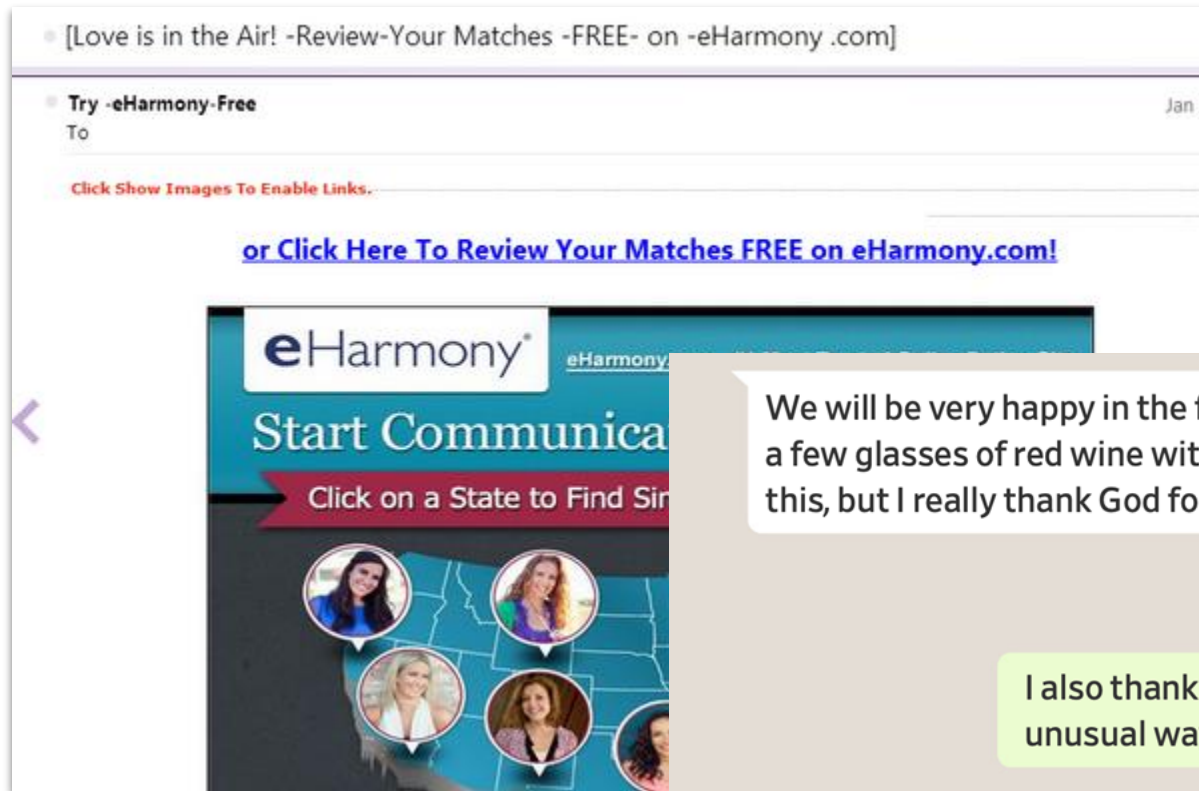
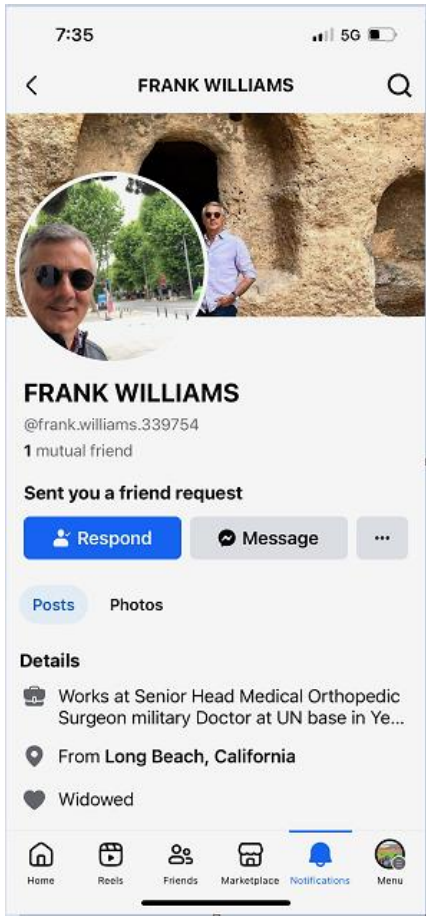
# Tech Support Crimes

- 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
  - Fraudulent 'Refund' where fraudster tells victims they are owed a refund for prior services, requiring a credit card, or
  - 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>





# Romance Scams



We will be very happy in the future, maybe because I had a few glasses of red wine with my friend, that's why I say this, but I really thank God for letting me meet you

I love you very much

I also thank God for having us come together in such an unusual way. I really believe we are meant for each other

I couldn't have found a more perfect woman than you. I am the luckiest man on earth to find you

# Romance Scams



We've detected a concerning pattern and wanted to check in

We've detected 5 instances of financial behavior that seemed out of character for you. Given the recent rise in scams, we just wanted to check in. Here are the transactions:

Sep 25 2022 **Wire Transfer**  
Chase Checking 1425

Sep 25 2022 **Crypto.com Purchase**  
Citi Preferred Checking 4B48

Sep 25 2022 **New Transfer Recipient**  
Chase Checking 1425

Sep 25 2022 **Potential Missed Bill**  
Chase Checking 1425

[See all transactions](#)

Here's some signs this might be an issue:

- 01 Someone you met online or through text messaging has begun to ask for money.
- 02 The person asking for money refuses to meet in person or makes excuses as to why they can't meet in person.
- 03 The person has provided account numbers, digital payment like Zelle or Venmo, or has asked for gift cards in order to receive money.

[Learn More](#)

[Get Help](#)

Was this alert useful?

## Related Articles



[Romance Scam Red Flags](#)

[Read](#)



[Safe Ways to Transfer Money](#)

[Read](#)

# Counterfeit Check Scams

- Cashier's checks and postal money orders can be forged. Cashier's checks are treated as guaranteed funds because the bank itself, rather than the individual account holder, is responsible for paying the amount of the check. Cashier's checks are commonly required for real estate and brokerage transactions. If a person deposits a cashier's check or money order, the person's bank must credit the account by at least \$5525 the next day.



<https://www.bbb.org/en/us/article/news-releases/18367-dont-cash-that-check-bbb-study-shows-how-fake-check-scams-bait-consumers>

# Counterfeit Check Scams

---

- Customer receives a check with instructions to deposit it in the bank
- Later asked to withdraw in cash and/or wire and/or Zelle
- The check is a fake, and is returned as counterfeit overdrawing the customer's account



## FAKE CHECK SCAMS

Did someone send you a check and ask you to send some money back?



### MAYBE:

You win a prize and are told to send back taxes and fees.

You get paid as a "secret shopper" and are told to wire back money.

You sold an item online and the buyer overpays.

### IN ALL CASES:



You get a check.



They ask you to send back money.



**THAT'S A SCAM.**

## FAKE CHECK SCAMS

Did someone send you a check and ask you to send some money back?

**THAT'S A SCAM!**



## FAKE CHECK SCAMS

If It's a Fake Check, Why Is Money in Your Account?  
Just because the check has cleared doesn't mean it's good!





AMERICAN RIVIERA  
BANK

# Solutions



# Solutions

- **Ensure Regulatory Compliance**
- **Technology solutions**
- **Educate account holders about fraud**
- **Develop an incident response plan**



# Evaluate your Processes

- Placing Holds
  - New Account
  - Large Deposit
  - Repeatedly Overdrawn
  - Redeposited Checks
  - Reasonable Cause to Doubt Collectability
  - Emergency Conditions
- Review Fraud Procedures
  - # of days to notify of fraudulent items
- Alternatives to writing checks
  - Positive Pay
  - ACH
- Training!

# Large Deposit Holds don't Protect Against Fraud

A large deposit hold only protects the bank if the check is returned before the end of the second business day.

In addition, it only works if a check is over \$5,525.

Client deposits a check from a business in the amount of \$12,000. You determine a hold will need to be placed. The bank must:

- Make \$225 available the next business day
- Make \$5,300 available on the second business day
- Make the remaining funds available on the seventh business day (\$6,475)



# Red Flags for Check Fraud

- Border, watermarks, holograms or other security features missing
- MICR line bold or raised compared to prior checks
- Erasures or alterations
- Relationship 30-60 days old

**KYC:** Source of funds not normal for client



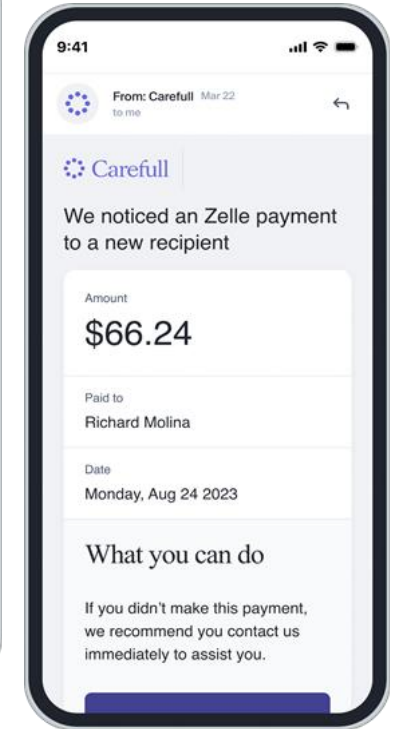
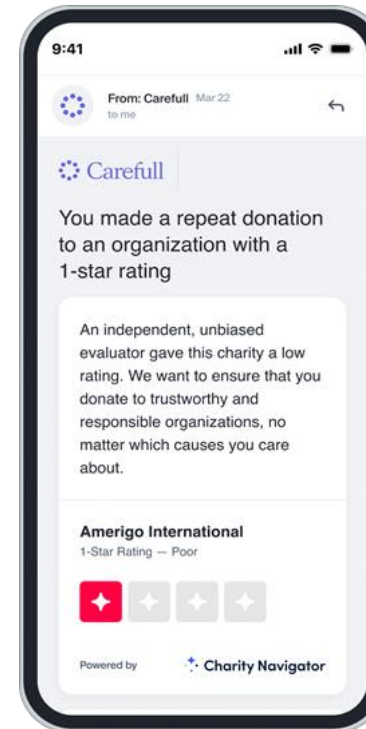
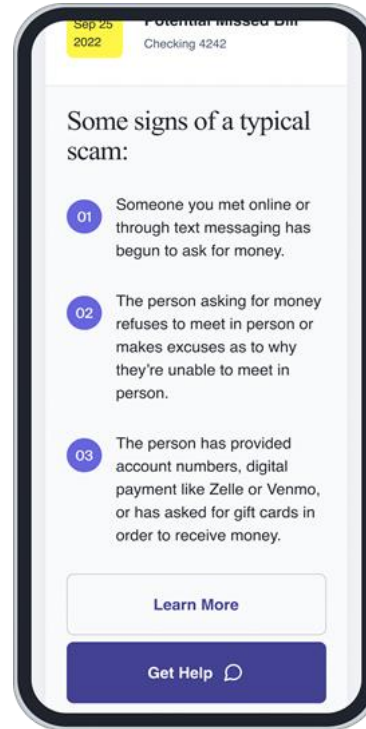
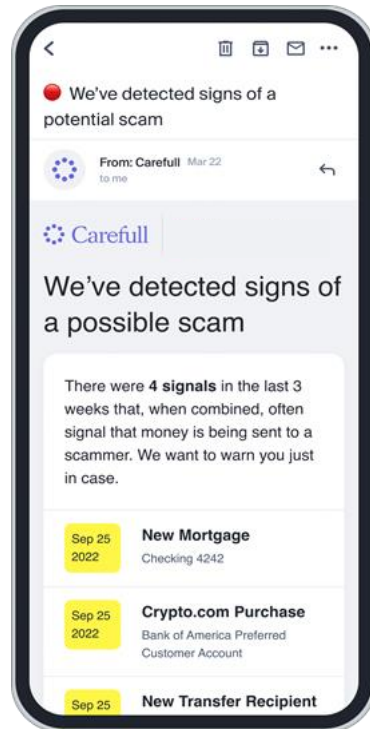
# Technology Solutions to Combat the problem

- 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



Cognitive Decline	Romance Exploitation	Elder Abuse	Unusual Behavior	Phishing Scams	Credit + Identity + Home
Recurring charity Reduced mobility Missed bills Duplicate services	New P2P recipient New crypto payment Dating site joined	Increased grocery bill Systemic drain	Strange check Strange ATM location High number of checks	Zelle Crypto Gift Card Bill Change	Change of address, new account opened, stolen email, stolen password

# Education and Resources

- Newsletters
- In Branch Posters
- Teller Counter Handouts
- Community Presentations



### RECOGNIZE THE SCAM

You get a call, email, or text message from someone claiming to be:

- BANK**: From your **BANK**, claiming they need to verify personal information before they can send you a new card.
- COURT OFFICIAL**: A **COURT OFFICIAL**, indicating that you failed to appear for jury duty and need to pay a fine or you will be arrested.
- POLICE**: The **POLICE**, saying you'll be arrested, fined or deported if you don't pay taxes or some other penalty.
- FAMILY**: A **FAMILY MEMBER**, a person saying your relative is sick, has been arrested or is in trouble and needs money.
- IRS**: From the **IRS**, saying you owe back taxes, there's a problem with your return or they need to verify information.

### PROTECT YOURSELF

Learn how to spot these scams and say no!

- BE VERY SUSPICIOUS**: Government agencies **DO NOT** call and ask for money or information ever.
- DON'T TRUST CALLER ID**: Even if it looks real, and says it's from a legit organization; it can be faked.
- NEVER PAY WITH...**: A wire transfer, money transfer app, crypto, or gift card. **THIS IS A SCAM.**
- ALWAYS CHECK FIRST**: Don't use the phone # they give you, look it up yourself. Call and find out if it's real.

# Resources for Clients



## AARP Fraud Victim Support Group

Experiencing fraud can be devastating, but you can recover from the trauma it causes.

[Subscri](#)

### About Us

#### Know that you are not alone

If you have been affected by a scam, the [AARP Fraud Watch Network™](#) offers free, confidential discussion groups for victims of fraud and their loved ones.

The **AARP Fraud Victim Support Group** provides individuals with an online forum to meet and interact with others who have experienced similar events. Our sessions are a safe environment to give and receive valuable feedback and support from others who are on the road to emotional healing and recovery.

Group sessions are **confidential** and led by trained facilitators who offer fraud education and understanding to participants, as well as time for meaningful peer-to-peer sharing and support.

#### Have Questions?

AARP Fraud Victim Support Group

Email: [fwn@aarp.org](mailto:fwn@aarp.org)

Telephone: 877-908-3360

[Visit website](#)



[Resource Library](#)



# Client-Facing Materials

Consider a checklist for the teller line to make them stop and think

## Is it a scam?

If you can answer “Yes” to any of these 10 questions, it’s a scam.

Hang up or do not interact with the message you have received.

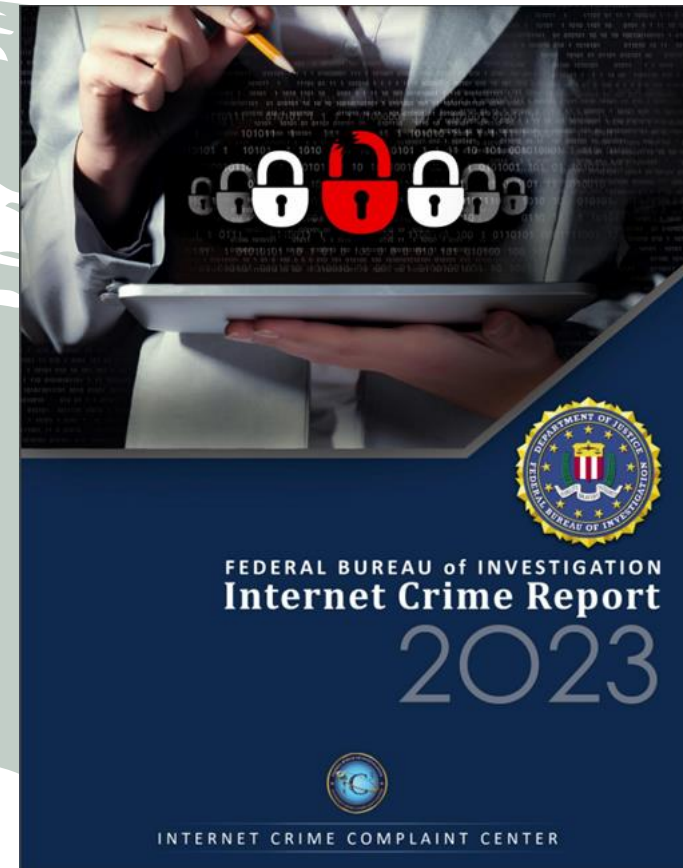
- 1 Did you receive a call, email or text message out of the blue from a government agency (IRS, FBI, Medicare, Social Security, etc.) or law enforcement asking for your personal information or a payment?
- 2 Did you get a text message or email from your bank, service provider, retailer or delivery service alerting you to a problem and asking you to click on a link or call a specific number?
- 3 Did you receive an unsolicited call, email or text message and are you being asked to make a payment with a wire transfer, gift card, prepaid card, cryptocurrency or payment app such as Zelle?
- 4 Did you get a pop-up message on your computer or a call telling you there is a problem with your computer and that you need to make a payment or grant someone remote access to your computer to fix it?
- 5 Are you being asked to pay a fee or provide personal information to collect sweepstakes or prize winnings?
- 6 Is someone asking you to stay on the phone with them as you make a withdrawal, purchase a gift card or transfer money and to not tell anyone what is happening?
- 7 Is someone offering you the opportunity to make an investment with a high return and little to no risk?
- 8 Is someone you’ve connected with through a job listing, email offer, social media, online marketplace or dating site asking you to deposit a check, keep some of the money and send some of the money back or to another account?
- 9 Did you get a call from a family member in trouble who is asking you to send money right away and to keep it a secret?
- 10 Did you develop a relationship with someone online who is unable to meet you in person and is asking for money?

# Front-Line Materials

<p><b>What is the check for?</b></p>	<p>If it appears suspicious (loan to pay medical debt, investment opportunity, a “friend”)</p> <p>Ask: how did you receive it?</p> <ul style="list-style-type: none"> <li>• If mail, report to USPIS and contact our local reps to determine whether the address is a known fraud address.</li> </ul> <p>Notify the client a hold will be placed. If they appear upset or “need to send money now”, that should be a red flag. <b>Zelle funds typically cannot be recalled after they are sent. Consider contacting digital.</b></p> <ul style="list-style-type: none"> <li>• You can offer to call to verify the check and release the hold</li> </ul>
<p><b>What is the purpose of the cash withdrawal?</b></p>	<p>If suspicious and drawn on uncollected funds probe further.</p> <p>Ask: Where are you taking the cash?</p> <ul style="list-style-type: none"> <li>• If Bitcoin ATM, report to the Secret Service.</li> <li>• If cash was mailed, report to USPIS.</li> <li>• If cash was used to buy gift cards, contact the company to determine if they have been redeemed.</li> </ul>
<p><b>Do you need access to this deposit immediately?</b></p>	<p>If yes, ask:</p> <ul style="list-style-type: none"> <li>• Who are you sending the money to?</li> <li>• How did you meet the person who gave you the check/asked you to send a wire/Zelle/buy the gift cards?</li> <li>• Did they warn you not to tell the bank or say “<b>it’s a private matter</b>”?</li> <li>• If yes, “This sounds like a scam. Let me send you some information to review before you speak to them again.”</li> </ul>
<p><b>Did you give out any personal information?</b></p>	<p>If yes</p> <ol style="list-style-type: none"> <li>1. Flag the account as Identity Theft and file a QAR with the details of the case.</li> <li>2. Have the client visit the IDtheft.gov checklist.</li> <li>3. Ask them whether they clicked on any links or allowed access to their computer.</li> </ol>
<p><b>Did they tell to go to a link or download anything?</b></p>	<p>If yes, these may contain malware or phishing attempts.</p> <p>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).</p>
<p><b>Did the person threaten legal action or to freeze your account?</b></p>	<p>If yes, ask if they have contact information for the person who contacted them.</p>

# Incident Response: 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





# Always Report in Addition to Filing SAR



- Cybercrimes – FBI  
<http://www.ic3.gov/default.aspx>



- File a Consumer Complaint  
<https://www.ftc.gov/>



- File Mail Fraud  
<https://www.uspis.gov/>





Thank You!

Questions?