

# **Staying Ahead of Fraud**

Trends in 2026

# PRESENTERS



**LAUREL SYKES, CRCM**

Laurel Sykes is EVP and  
Chief Risk Officer American  
Riviera Bank



**Jennie Bailey, CAMS, CFE**

Jennie Bailey is VP and  
Director of the FIU at  
Tri Counties Bank



1 Fraud targeting business clients

---

2 Enhanced due diligence

---

3 Bank impersonation scams

---

4 Fraud targeting older clients

---

5 Victim response and prevention

---



## **Business Identity Theft**

Corporate filings and accounts created to impersonate a legitimate company

## **Payment Diversion**

Vendor invoices, payroll changes, and wire instructions

## **Business Email Compromise**

Impersonation through compromised or lookalike email

## **Check Fraud**

Stolen, altered, counterfeit, or misdirected checks



# How Business Identity Theft Happens

BUSINESS IDENTITY THEFT

1

## Select

Scammers identify a legitimate business with a strong reputation.

2

## Create

They register a similar business name in another state and obtain an EIN.

3

## Open

They use the new filing and EIN to open a bank account.

4

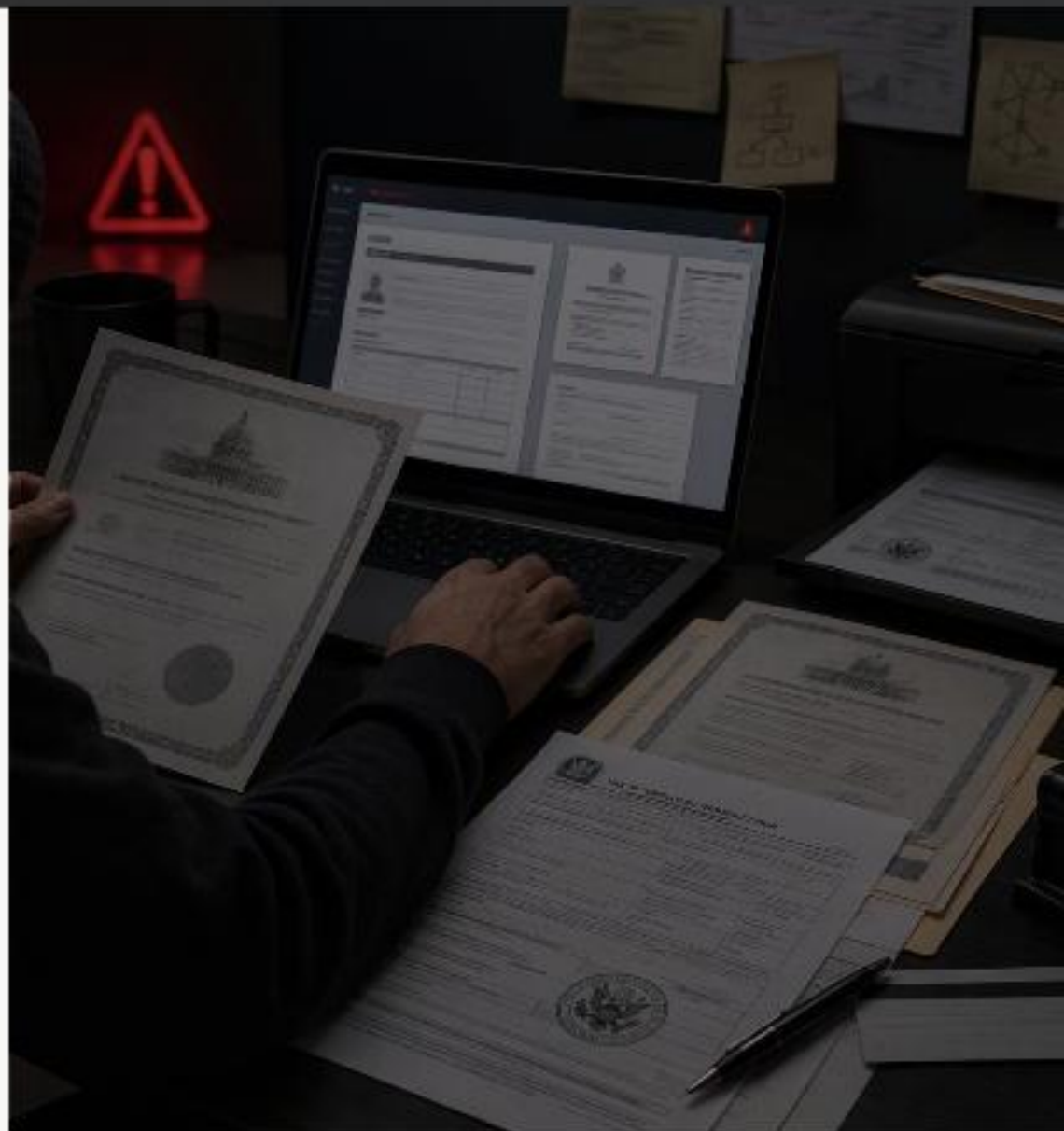
## Exploit

Then they deposit stolen checks or redirect payments intended for the real business.

5

## Exit

Move funds quickly through cash, wire, or cryptocurrency.





**Very recent registration** Entity formed within days, sometimes the same week as account opening.

**Out-of-state formation** New entity formed elsewhere while claiming expansion into California.

**Near-match business name** Abbreviation, altered punctuation, or LLC used instead of Inc.

**Out-of-state organizer or officer** Identification and stated business footprint do not align.

**Thin operating evidence** Limited support for the claimed expansion, location, clients, or vendors.

# Questionable Account Activity

TRANSACTION MONITORING

- Large check payable to the business with an out-of-state address.
- Check issued before the business was registered.
- Large incoming ACH credits from unrelated companies.
- Significant check deposits shortly after account opening.
- Interstate wire activity inconsistent with stated operations.
- High-velocity movement of funds.



**Pattern matters: new entity + unusual deposit + rapid exit.**



| Verify the entity                                                                                                                                                                                                                                                    | Verify the people                                                                                                                                                                                                                        | Verify operations                                                                                                                                                                                                                                        |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• Search the formation state and California Secretary of State websites.</li><li>• Compare legal name, entity type, formation date, status, and officers.</li><li>• Look for similar or nearly identical businesses.</li></ul> | <ul style="list-style-type: none"><li>• Research managers, officers, and organizers independently.</li><li>• Confirm authority to act for the business.</li><li>• Reconcile residence, business location, and expansion story.</li></ul> | <ul style="list-style-type: none"><li>• Validate website, address, phone, licensing, and commercial footprint.</li><li>• Request documents supporting the California expansion.</li><li>• Escalate unexplained inconsistencies before opening.</li></ul> |

**Pause the opening when the filing, people, and operating story do not align.**

# Business Email Compromise

- Impersonation through email compromise
  - Impersonating clients
  - Business impersonation via email from someone who appears to be within the company
- Fake documents, surveys, encrypted email to introduce malware or collect credentials

Jeff DeVine  
OFFICE TASKS

To: honak@americantiviera.bank  
Bcc: honak@arb.bank  
Sent On: Tuesday, January 7, 2025 7:15:02 PM  
Archived On: Tuesday, January 7, 2025 7:16:08 PM  
Identification Code: eml:04c6616d-8cdf-433d-8fa8-051d4e76ea06-2147459940

---

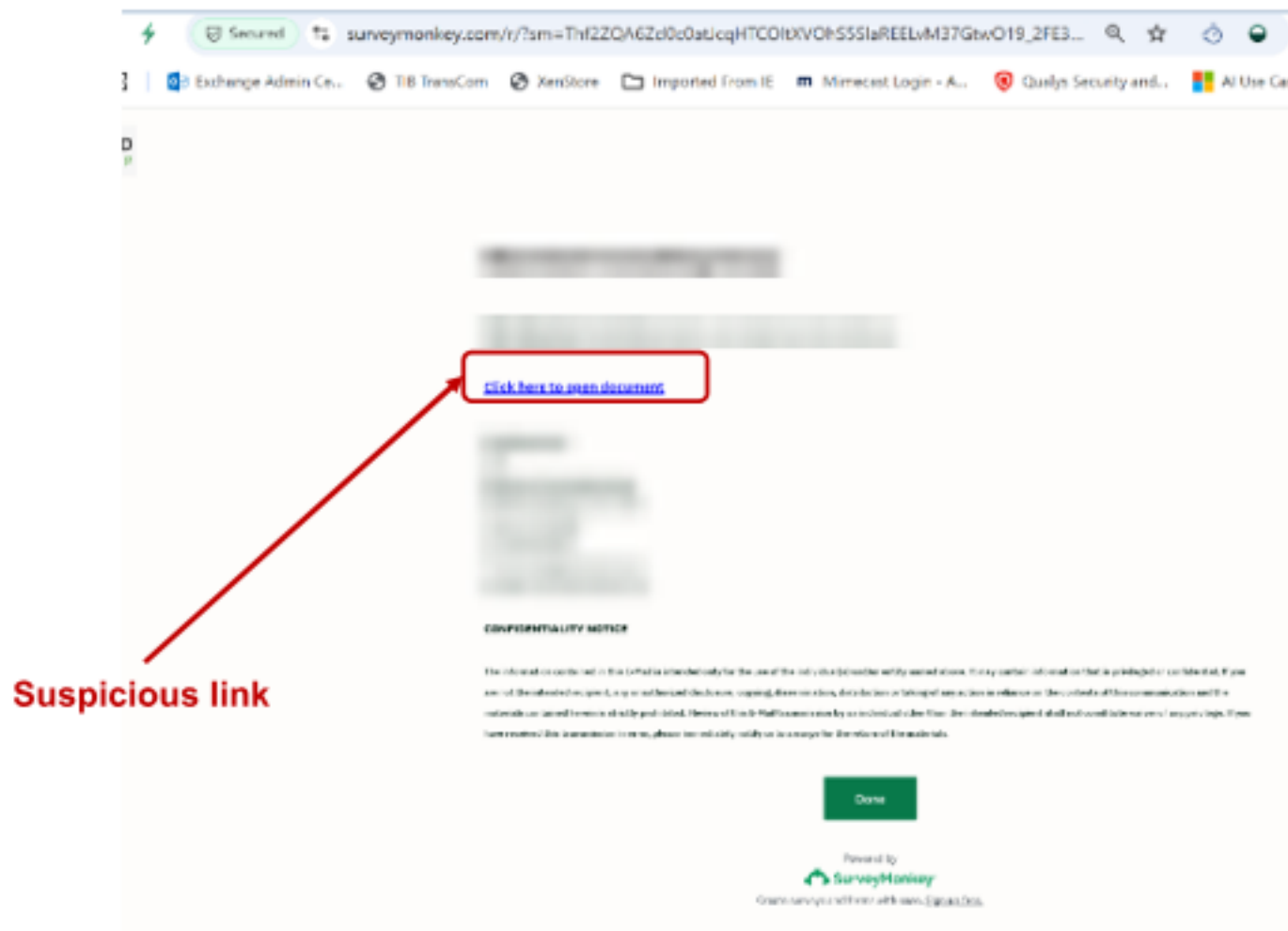
This message is external. The message is from: officehtasks@gmail.com

---

Dear Holly  
Kindly re-affirm your direct cell and lookout for my text.

BEST REGARDS!

# Malicious Links in Email



One click can install malware or open a credential-stealing page

Links are hidden in invoices, shared-file notices, and password-reset alerts

Lookalike domains and URL shorteners disguise the true destination

One compromised device can expose the network and customer data

Hover before clicking, verify the sender, report suspicious mail

# Vendor Invoice Scams

**From:** s.rollins@coachhub.com

**Sent:** Monday, September 21, 2026 3:16 PM

**To:** ARB Client <email@email.com>

**Subject:** Invoice Due for Payment

As discussed during our recent call, I am writing to formally request a status update regarding the attached invoice, which is now due for payment. Please let us know if there are any additional details or documentation your team requires to facilitate prompt payment.

Thank you in advance for your timely assistance.

Best regards,

Sandra Rollins

Leadership Development Coach @CoachHub

Coaching, Leadership Development

447 Broadway, 2nd FL, New York, 10013

# Detecting Check Fraud

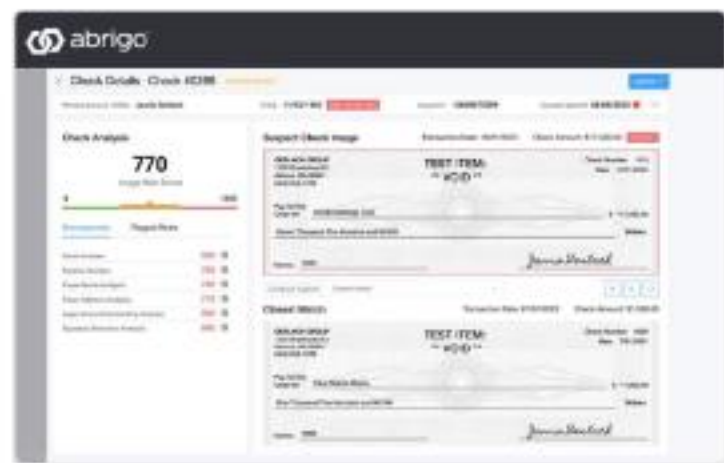
## Check Analysis

### Image Analysis

Payor name  
Payor Address block  
Payee name field  
Payee Handwriting Style  
TO THE ORDER OF keyword  
Structural layout  
Reduced image of whole check  
Signature detection  
Legal amount field  
Courtesy amount field  
MICR line

### Security features

Borders  
LAR handwriting style  
Date keyword  
Courtesy sign  
Check number field  
Date field  
Comparison of check number  
CAR/LAR difference  
LAR printed font case  
LAR printed text style  
Printed payee font case  
Printed payee text style  
Payee name handwriting style

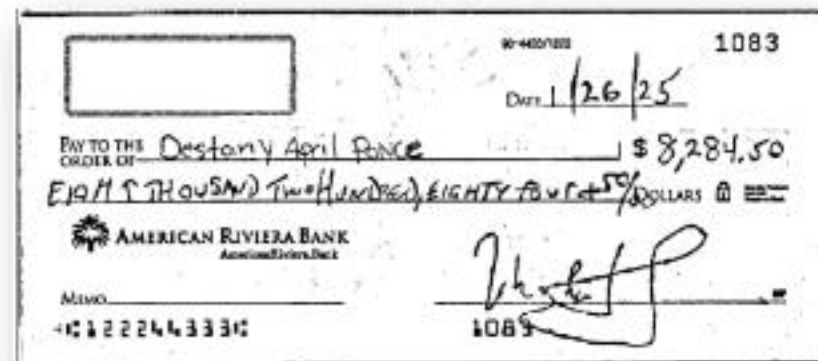


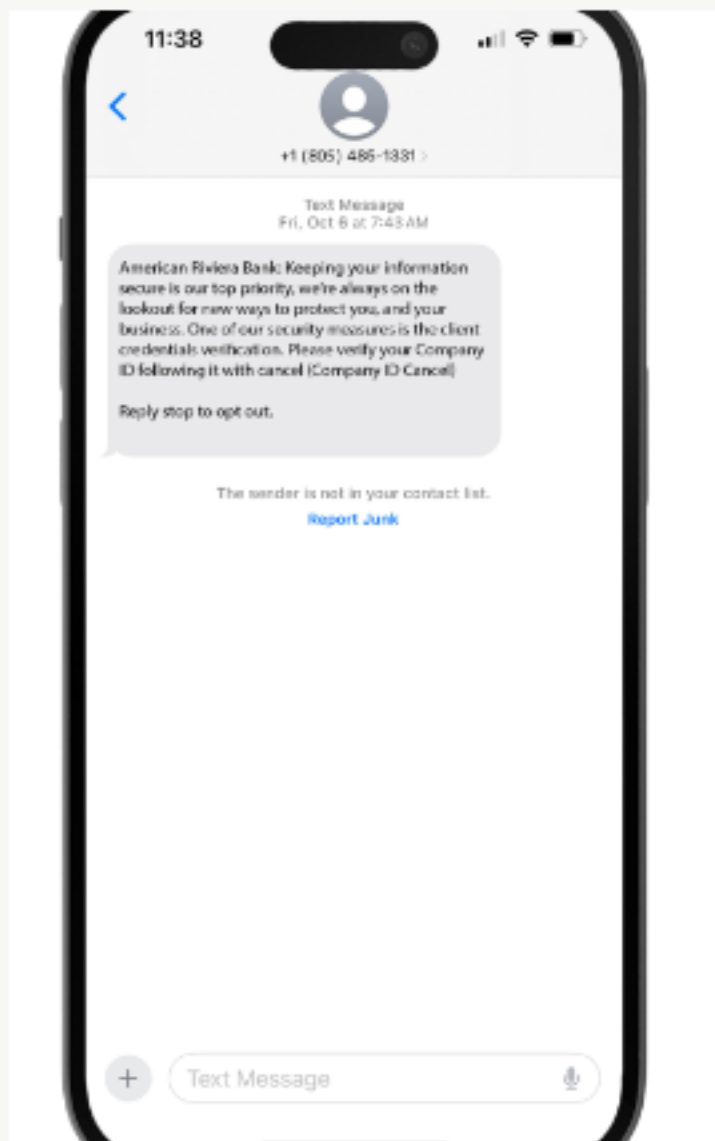
Other Data Sets:  
v Flagged rules  
v Closest match capability  
v Cleared check history

## Counterfeit Check



## Altered Check





1

**A call or text appears to come from the bank.**

Caller ID may be spoofed to resemble an official number.

2

**The message asks about an unauthorized transaction.**

The criminal offers technical support for a supposedly compromised account.

3

**The customer is asked for credentials or a security code.**

The code sent to the mobile device can be used to take control of the account.

4

**Account access and payment settings are changed.**

The criminal may change the phone number, add Zelle payees, or initiate external transfers.

**Banks never ask customers to provide passcodes or PINs.**

# Financial Crimes Targeting Older Clients



---

Investment Scams/Crypto

---

Phone/Text Impersonations

---

Tech Support Scams

---

Mass Mail Scams

---

Romance/Relationship Scams

---

Counterfeit Check Scams

---

Compromised Email Accounts



## **Notify stakeholders**

Tell customers, vendors, and partners that the business is being impersonated.



## **Reconfirm payment channels**

Provide valid contact information and require independent verification of payment-instruction changes.



## **Monitor the internet**

Search daily for fraudulent websites and social media pages using the business name.



## **File a police report**

Document the incident and preserve filings, communications, payment details, and screenshots.



## **Brief employees**

Reinforce vigilance around links, credential phishing, and impersonation attempts.

**Use known, independently verified contact information, not contact details supplied in a suspicious message.**



## Protect access

- Use multi-factor authentication for email and banking.
- Use unique passwords for banking and higher-risk systems.
- Examine sender addresses, domains, and links.
- Do not rely on caller ID or an email thread alone.

## Protect payments

- Require dual approval for payment-instruction changes.
- Verify changes through a known phone number.
- Use Positive Pay, alerts, card controls, and fraud-protection tools.
- Train employees to report suspicious messages quickly.

**Slow down, verify independently, and escalate inconsistencies.**

# Resources for Prevention



## Online Banking Tools

- Positive Pay for Businesses
- Online Banking Alerts
- Fraud Protection Services
  - Dark Web Monitoring
  - ID Theft Insurance
- Card controls

## For Phones

- Forward texts to 7726
- Call blocking
  - For videos: <https://www.fcc.gov/call-blocking>
  - For links to apps: <https://www.ctia.org/consumer-resources/how-to-stop-robocalls>

## Anti-malware and Anti-remote tools

# Resources for Business Clients

[Business](#) - [Personal](#) - [About](#) - [Resources & Tools](#) -

[Contact](#) [Locations](#) [Investor Relations](#) [Sign On](#) 



## Business Fraud Toolkit

Practical steps to prevent fraud and respond fast.

Take Action!

[Report Suspected Fraud](#)

[Contact Support](#)

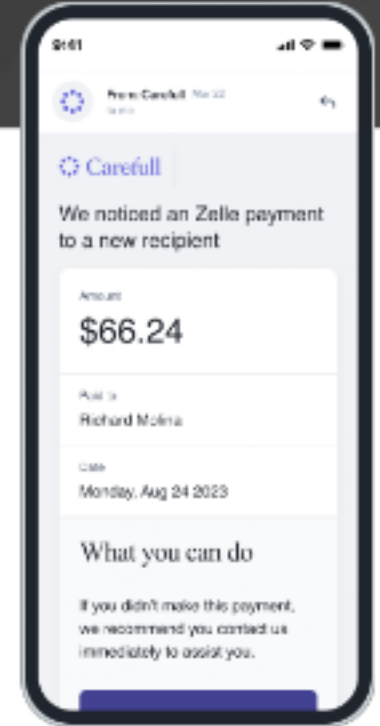
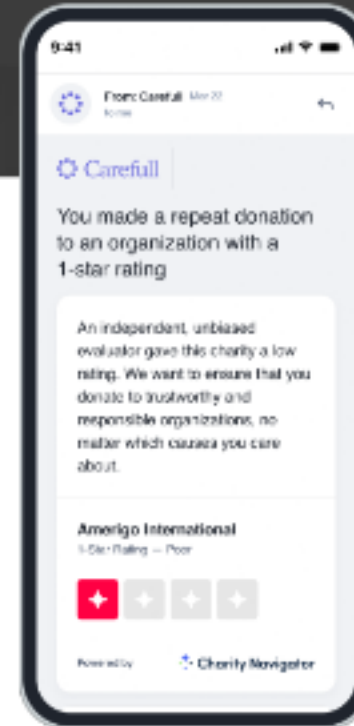
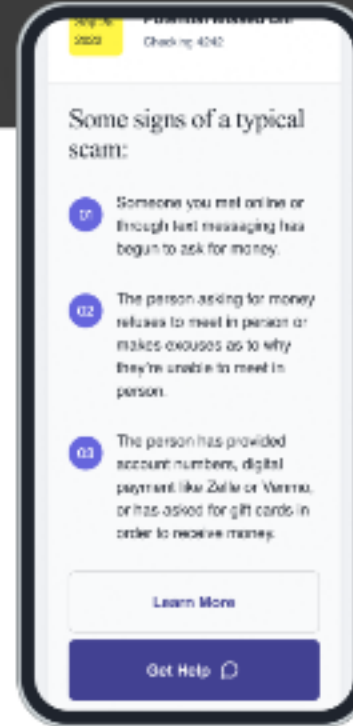
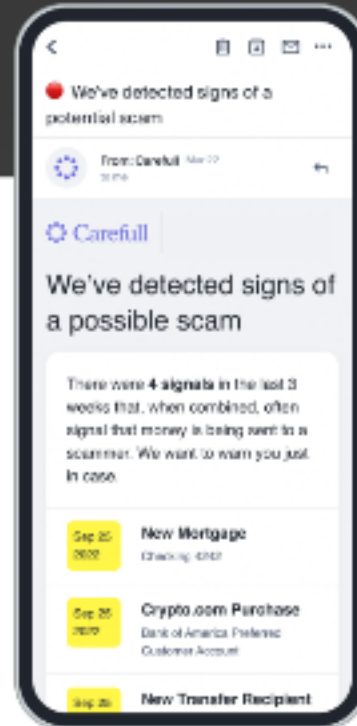
On this page: [Trending Threats](#) [How Fraud Works](#) [Recognize the Scam](#) [Prevention Checklist](#) [Resources](#) [FAQs](#)

### Trending Threats

#### Bank Impersonation Scams

This scam occurs when a fraudster pretends to be from your financial institution and contacts you by phone, email, or text claiming there is a problem with your account. The scammer then pressures you to "verify" information such as login credentials, account numbers, or a one-time password.

- You receive a call about a "suspicious" transaction from someone claiming to be the bank's fraud department
- The caller claims that to stop the transaction, you must provide your credentials and the one-time passcode sent to your phone
- You are pressured to act immediately to "protect your accounts"



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



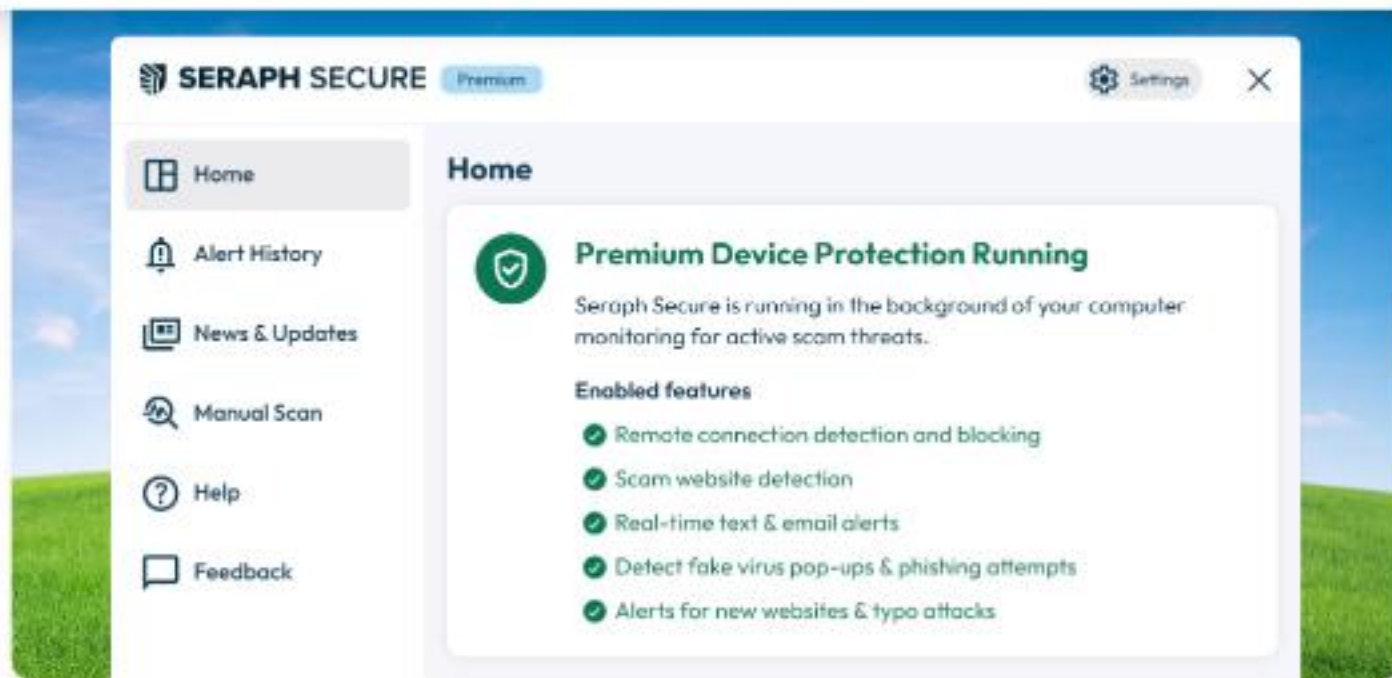
## Act quickly

- Call the receiving bank right away to freeze accounts and stop payments.
- File a complaint with the FBI at [ic3.gov](https://ic3.gov).
- Report fraud at [ReportFraud.ftc.gov](https://ReportFraud.ftc.gov) and [IdentityTheft.gov](https://IdentityTheft.gov).
- Encourage client to file a local police report for documentation.

## Victim support

- Place a fraud alert or credit freeze with all three bureaus.
- Change passwords and turn on multi-factor authentication.
- Elder Fraud Hotline: 1-833-FRAUD-11 (1-833-372-8311).
- Contact Adult Protective Services if exploitation is suspected.

**Keep records of all calls, messages, and transactions.**



Proactively prevent scams from taking place, protect family members, and safeguard personal information with Seraph Secure.

### As seen on



Bloomberg



#### Remote Access

Blocks remote software scammers use to gain access to your device.



#### Scam Websites

Blocks thousands of known scam websites.



#### Fake Virus Pop-ups

Detects deceptive virus pop-up messages.



#### Phishing Links

Detects and blocks malicious links from emails and ads.

**Questions?**