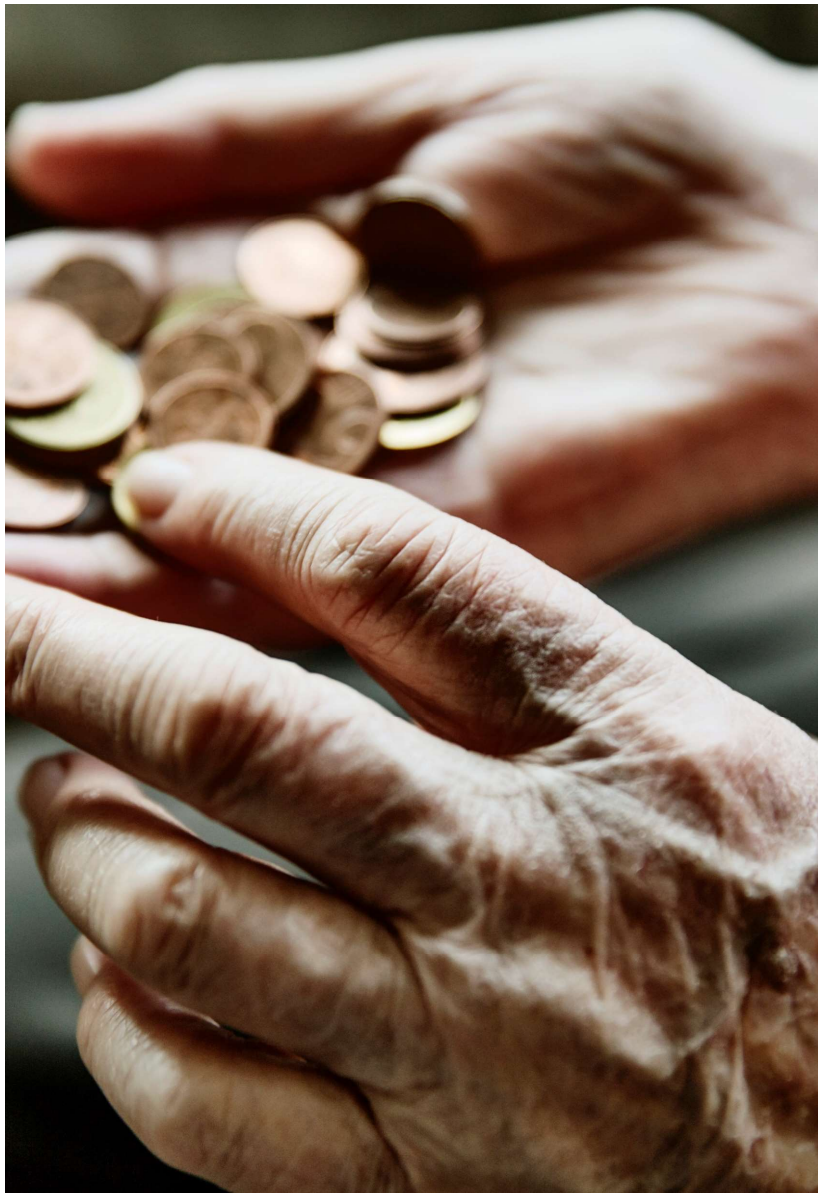
Identifying and Protecting Victims of Financial Crime

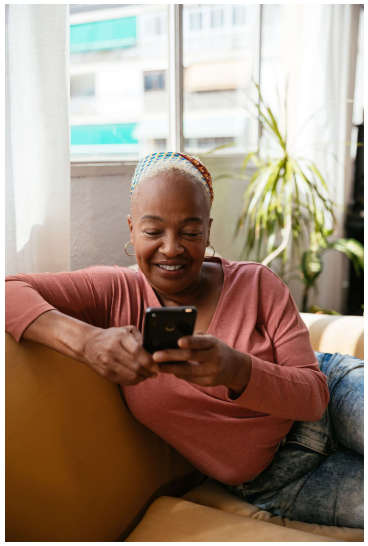
AMERICAN RIVIERA BANK
Bank on *better.*

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 453,000 cyber-enabled fraud complaints, with reported losses exceeding $17.7 billion in 2025, according to the latest IC3 report
  - Highest losses were comprised of ~~149,686~~ 181,565 complaints of cyber-enabled crime and fraud involving cryptocurrency, with over ~~**$9.3 billion**~~ **$11 billion in reported losses**
- Transnational Scam Centers
- Multi-tiered scams involving bank or law enforcement impersonations
- Scams that target bank employees



WHY IT'S WORKING



COVID was an accelerator. 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

AGENDA

TRANSNATIONAL FINANCIAL CRIMES

AI AND EMERGING TRENDS

EFFECTIVE REPORTING TO GET RESULTS

TECHNOLOGY

FINAL TIPS & TAKEAWAYS

PRESS RELEASES

Treasury Sanctions Burma Armed Group and Companies Linked to Organized Crime Targeting Americans

November 12, 2025

HAOTAI INTERNATIONAL GROUP

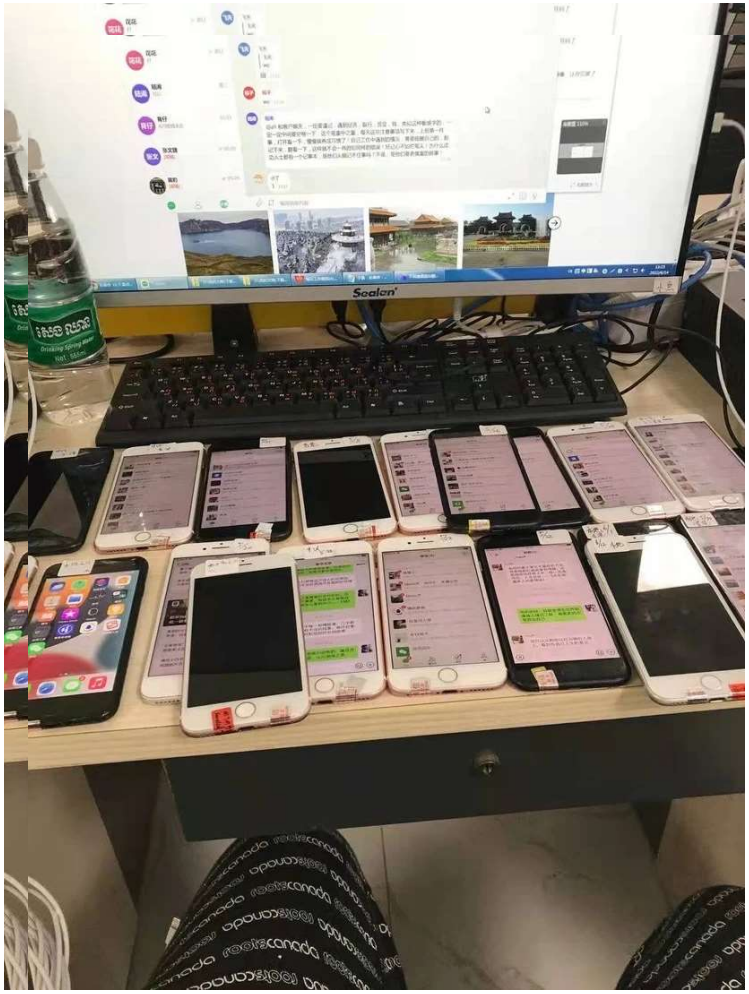
HOME JOBS ROADMAP CONTACT US Select Language

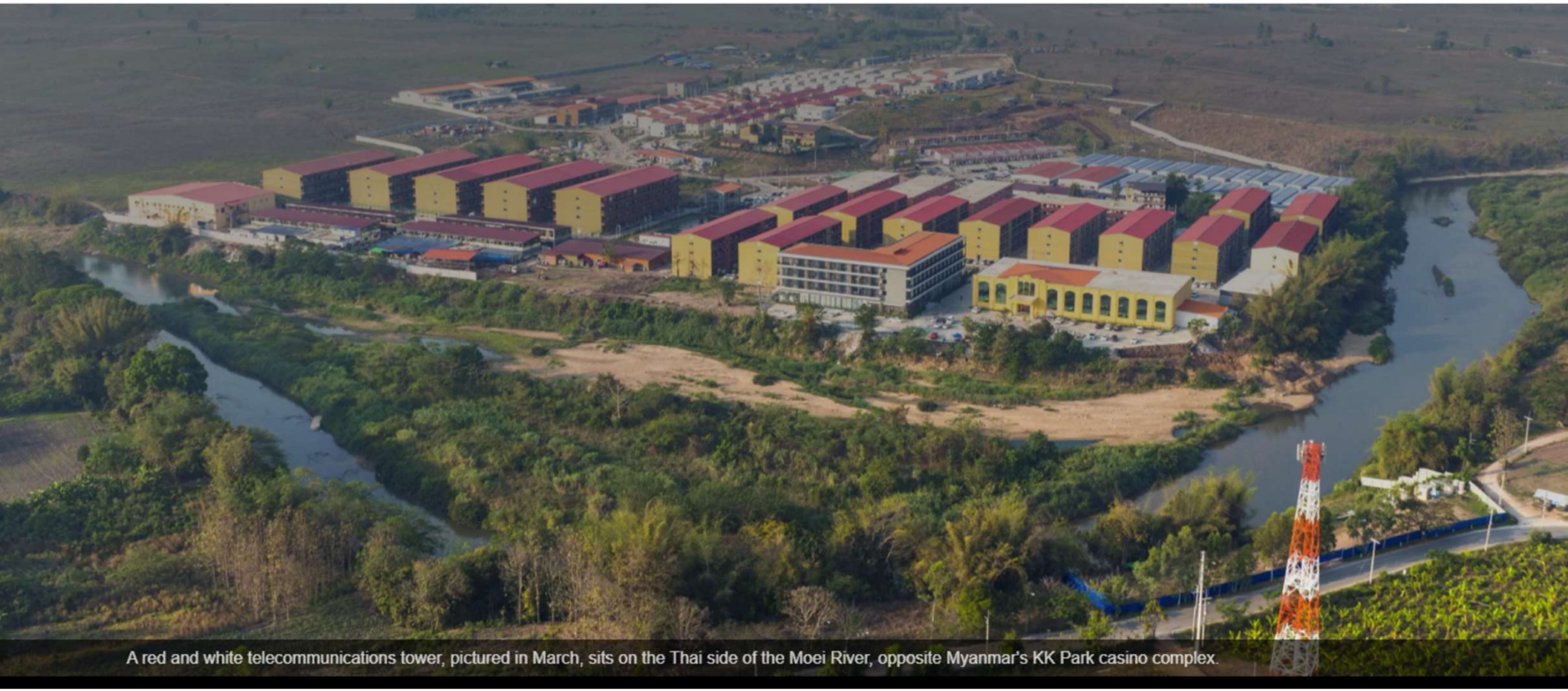
HAOTAI

HAOTAI INTERNATIONAL GROUP a partner of Asia's top financial and crypto group, currently one of the few overseas financial operating companies, From 2015 to 2022, it won unanimous praise in the industry and a number of technical patents and completed the top ten outstanding performance indicators in Asia Accompanying international financial markets.

In response to the technological and financial development of the times, in 2018 the company invested heavily to build a technology industrial park, ad 'TECH PARK' further study industry technologies and recruit talents for the global market It plans to attain the leading honor in the Asian financial industry in upcoming days. The company's main business is blockchain technology application and research and development, overseas financial investment and financial consulting, business information, software research, and development, electronic trading of bulk commodities, overseas physical trade operations, etc.

We expanded our business in many countries main branch in Thailand maesot. We expanded our business to Dubai, Vietnam, China, Singapore, Malaysia Activities of our company product based (Digital Currency) with 16,000 Employees working. Our Tech Park held in 750 acer's area.


Scalon



A red and white telecommunications tower, pictured in March, sits on the Thai side of the Moei River, opposite Myanmar's KK Park casino complex.


MAXAR
Moei river
Feb 2020 —— Sept 2023
Source: Maxar

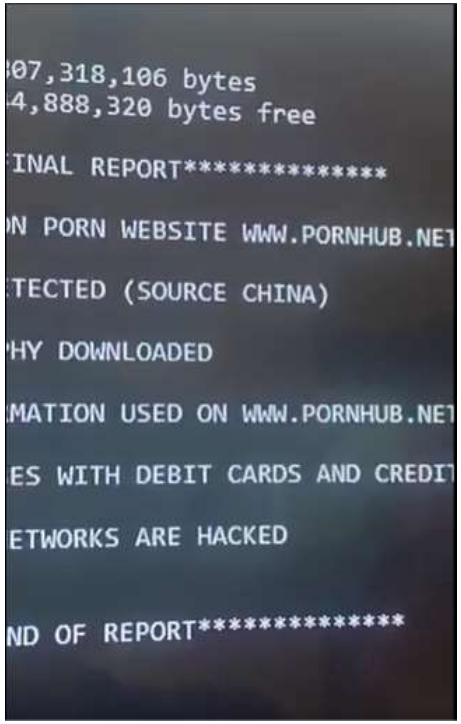
PHANTOM HACKER CRIMES

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

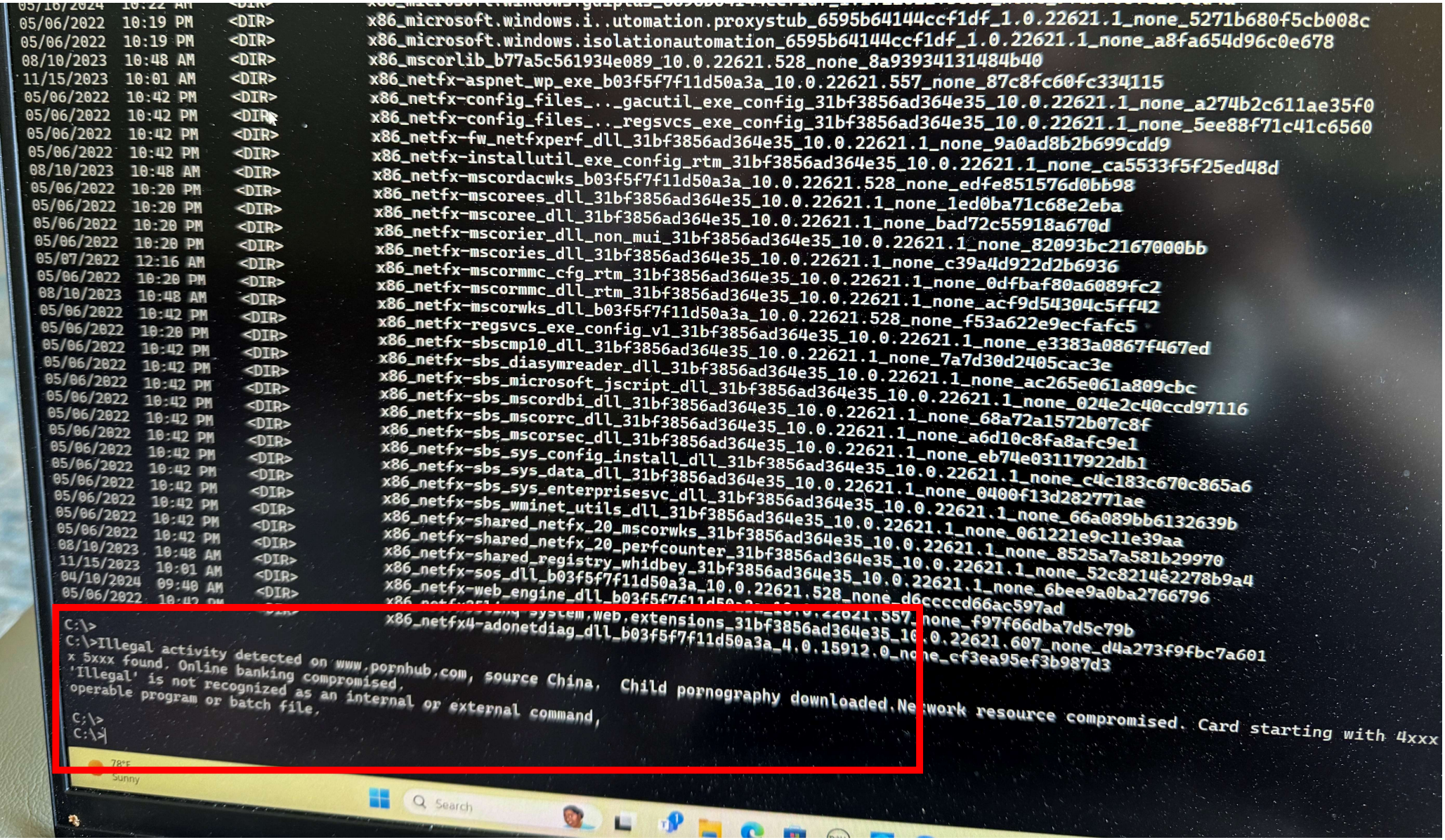
A popup window says your computer is at risk. The message in the window warns of a security issue on the computer and to call a number to get help.

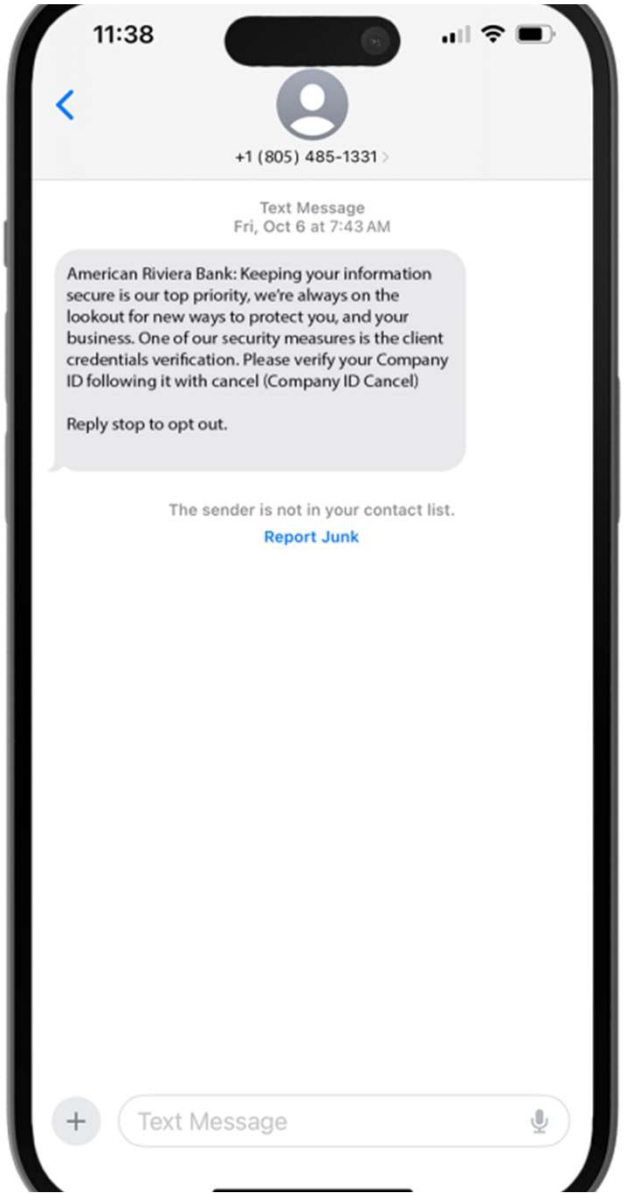
1. Fraudulent 'Refund' where fraudster tells victims they are owed a refund for prior services, requiring a credit card, or
2. Ransomware- fraudster installs malware that holds your computer 'hostage' demanding money for access.

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



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


05/06/2022 10:19 PM <DIR> x86_microsoft.windows.i..utomation.proxystub_6595b64144ccf1df_1.0.22621.1_none_5271b680f5cb008c
05/06/2022 10:19 PM <DIR> x86_microsoft.windows.isolationautomation_6595b64144ccf1df_1.0.22621.1_none_a8fa654d96c0e678
08/10/2023 10:48 AM <DIR> x86_mscorlib_b77a5c561934e089_10.0.22621.528_none_8a939341314846b40
11/15/2023 10:01 AM <DIR> x86_netfx-aspnet_wp_exe_b03f5f7f11d50a3a_10.0.22621.557_none_87c8fc60fc334115
05/06/2022 10:42 PM <DIR> x86_netfx-config_files_..._gacutil_exe_config_31bf3856ad364e35_10.0.22621.1_none_a274b2c611ae35f0
05/06/2022 10:42 PM <DIR> x86_netfx-config_files_..._regsvcs_exe_config_31bf3856ad364e35_10.0.22621.1_none_5ee88f71c41c6560
05/06/2022 10:42 PM <DIR> x86_netfx-fw_netfxperf_dll_31bf3856ad364e35_10.0.22621.1_none_9a0ad8b2b699cdd9
05/06/2022 10:42 PM <DIR> x86_netfx-installutil_exe_config_rtm_31bf3856ad364e35_10.0.22621.1_none_ca5533f5f25ed48d
08/10/2023 10:48 AM <DIR> x86_netfx-mscordacwks_b03f5f7f11d50a3a_10.0.22621.528_none_edfe851576d0bb98
05/06/2022 10:20 PM <DIR> x86_netfx-mscorees_dll_31bf3856ad364e35_10.0.22621.1_none_1ed0ba71c68e2eba
05/06/2022 10:20 PM <DIR> x86_netfx-mscoree_dll_31bf3856ad364e35_10.0.22621.1_none_bad72c55918a670d
05/06/2022 10:20 PM <DIR> x86_netfx-mscorier_dll_non_mui_31bf3856ad364e35_10.0.22621.1_none_82093bc2167000bb
05/06/2022 10:20 PM <DIR> x86_netfx-mscories_dll_31bf3856ad364e35_10.0.22621.1_none_c39a4d922d2b6936
05/07/2022 12:16 AM <DIR> x86_netfx-mscormmc_cfg_rtm_31bf3856ad364e35_10.0.22621.1_none_0dfbaf80a6089fc2
05/06/2022 10:20 PM <DIR> x86_netfx-mscormmc_dll_rtm_31bf3856ad364e35_10.0.22621.1_none_acf9d54304c5ff42
08/10/2023 10:48 AM <DIR> x86_netfx-mscorwks_dll_b03f5f7f11d50a3a_10.0.22621.528_none_f53a622e9ecfafc5
05/06/2022 10:42 PM <DIR> x86_netfx-regsvcs_exe_config_v1_31bf3856ad364e35_10.0.22621.1_none_e3383a0867f467ed
05/06/2022 10:20 PM <DIR> x86_netfx-sbscmp10_dll_31bf3856ad364e35_10.0.22621.1_none_7a7d30d2405cac3e
05/06/2022 10:42 PM <DIR> x86_netfx-sbs_diasymreader_dll_31bf3856ad364e35_10.0.22621.1_none_ac265e061a809cbc
05/06/2022 10:42 PM <DIR> x86_netfx-sbs_microsoft_jscript_dll_31bf3856ad364e35_10.0.22621.1_none_024e2c40ccd97116
05/06/2022 10:42 PM <DIR> x86_netfx-sbs_mscordbi_dll_31bf3856ad364e35_10.0.22621.1_none_68a72a1572b07c8f
05/06/2022 10:42 PM <DIR> x86_netfx-sbs_mscorrc_dll_31bf3856ad364e35_10.0.22621.1_none_a6d10c8fa8afc9e1
05/06/2022 10:42 PM <DIR> x86_netfx-sbs_mscorsec_dll_31bf3856ad364e35_10.0.22621.1_none_eb74e03117922db1
05/06/2022 10:42 PM <DIR> x86_netfx-sbs_sys_config_install_dll_31bf3856ad364e35_10.0.22621.1_none_c4c183c670c865a6
05/06/2022 10:42 PM <DIR> x86_netfx-sbs_sys_data_dll_31bf3856ad364e35_10.0.22621.1_none_0400f13d282771ae
05/06/2022 10:42 PM <DIR> x86_netfx-sbs_sys_enterprisesvc_dll_31bf3856ad364e35_10.0.22621.1_none_66a089bb6132639b
05/06/2022 10:42 PM <DIR> x86_netfx-sbs_wminet_utils_dll_31bf3856ad364e35_10.0.22621.1_none_061221e9c11e39aa
05/06/2022 10:42 PM <DIR> x86_netfx-shared_netfx_20_mscorwks_31bf3856ad364e35_10.0.22621.1_none_8525a7a581b29970
08/10/2023 10:48 AM <DIR> x86_netfx-shared_netfx_20_perfcounter_31bf3856ad364e35_10.0.22621.1_none_52c8214e2278b9a4
11/15/2023 10:01 AM <DIR> x86_netfx-shared_registry_whidbey_31bf3856ad364e35_10.0.22621.1_none_6bee9a0ba2766796
04/10/2024 09:40 AM <DIR> x86_netfx-sos_dll_b03f5f7f11d50a3a_10.0.22621.528_none_d6ccccd66ac597ad
05/06/2022 10:42 PM <DIR> x86_netfx-web_engine_dll_b03f5f7f11d50a3a_10.0.22621.557_none_f97f66dba7d5c79b
x86_netfx4-adonetdiag_dll_b03f5f7f11d50a3a_4.0.15912.0_none_cf3ea95ef3b987d3
C:\>
C:\>Illegal activity detected on www.pornhub.com, source China. Child pornography downloaded.Network resource compromised. Card starting with 4xxx
x 5xxx found. Online banking compromised.
'Illegal' is not recognized as an internal or external command,
operable program or batch file.
C:\>
C:\>
78°F
Sunny
Search

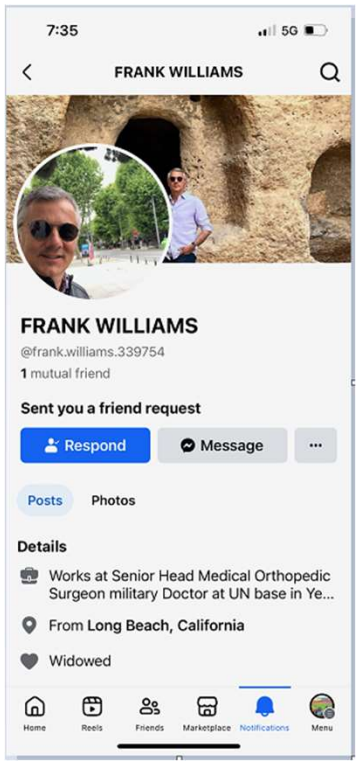


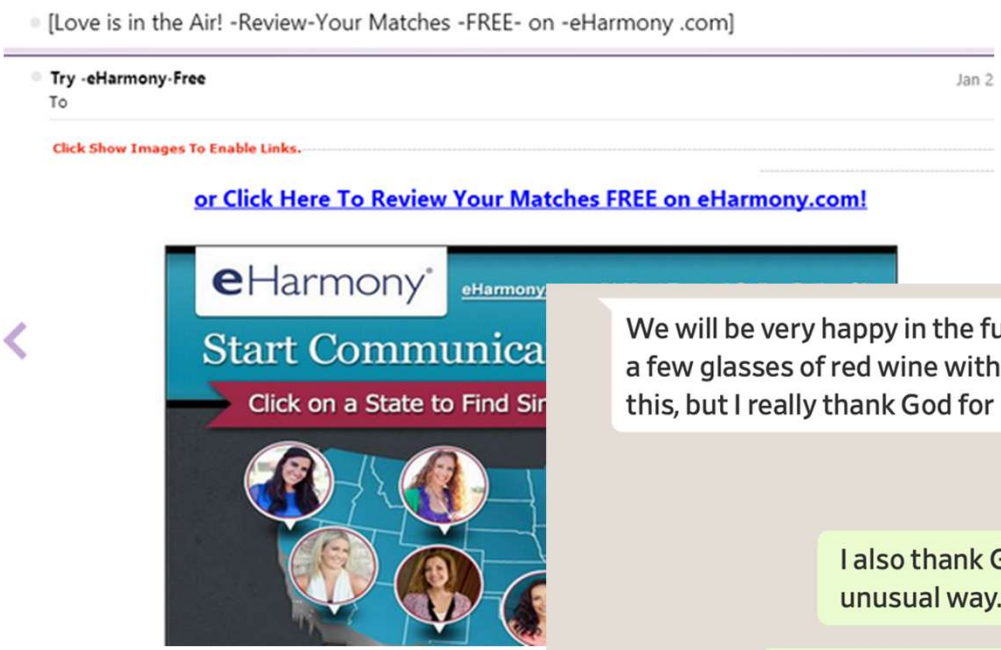
BANK IMPERSONATIONS

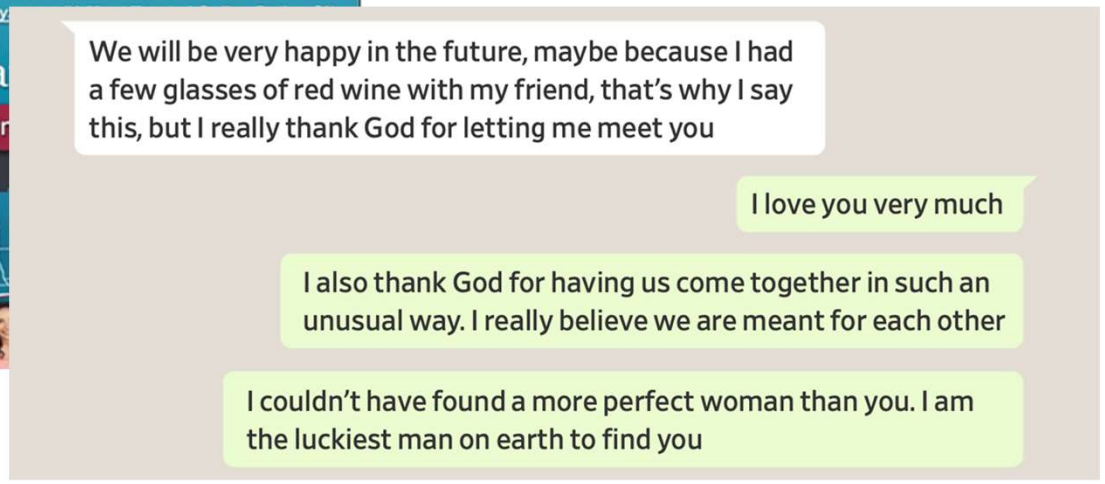
New trend away from suspicious debit card transactions to credential theft

- 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

ROMANCE SCAMS







ROMANCE SCAMS

Carefull

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 4848
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?

Yes | No

Related Articles

Romance Scam Red Flags

Read

Safe Ways to Transfer Money

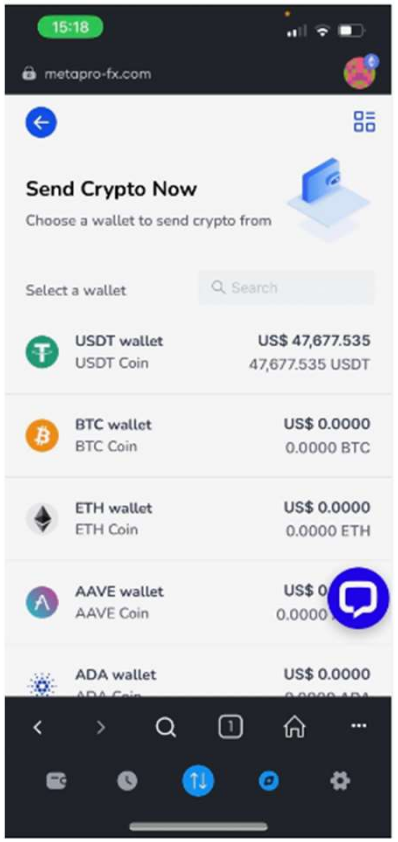
Read

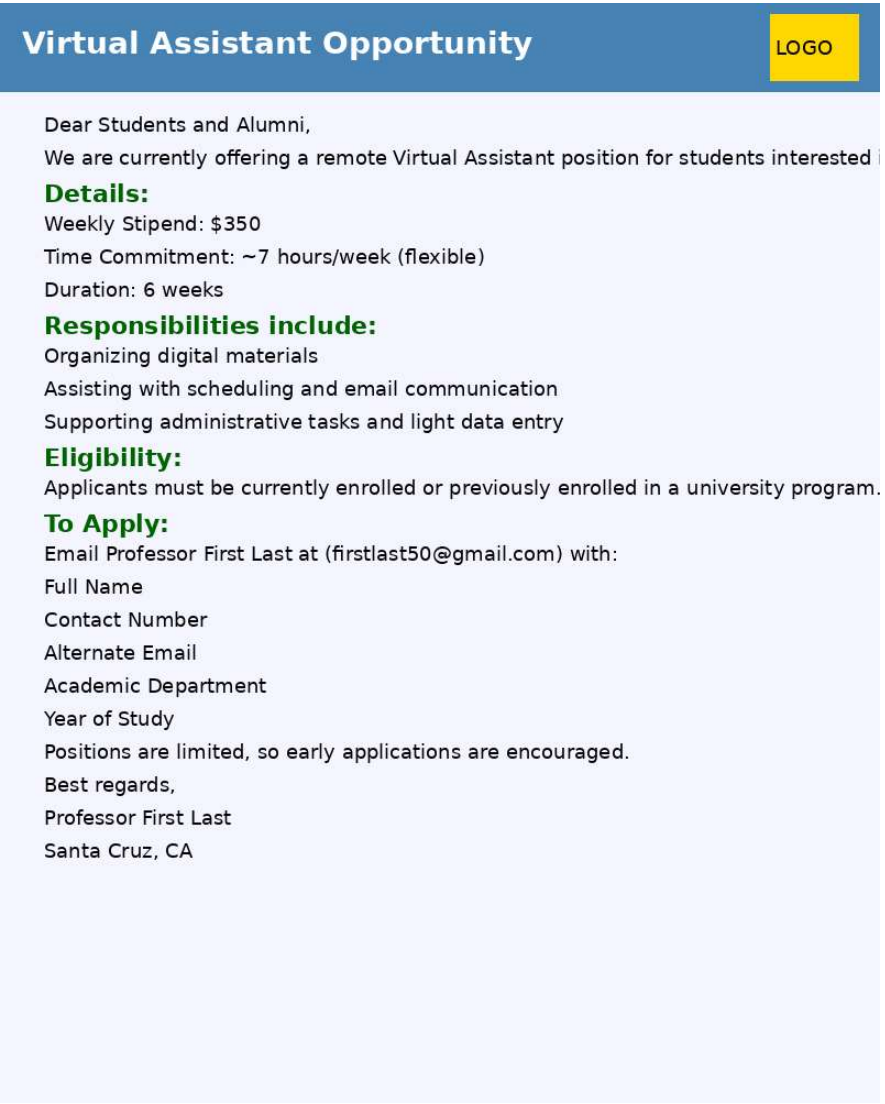
INVESTMENT SCAMS / PIG BUTCHERING

CONNECT WITH SOMEONE ONLINE OR BY TEXT

THEY ASK YOU TO INVEST

THEY SHOW YOU "PROFITS"





Virtual Assistant Opportunity LOGO

Dear Students and Alumni,

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

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

Offer for employment for a Virtual Remote Assistant job

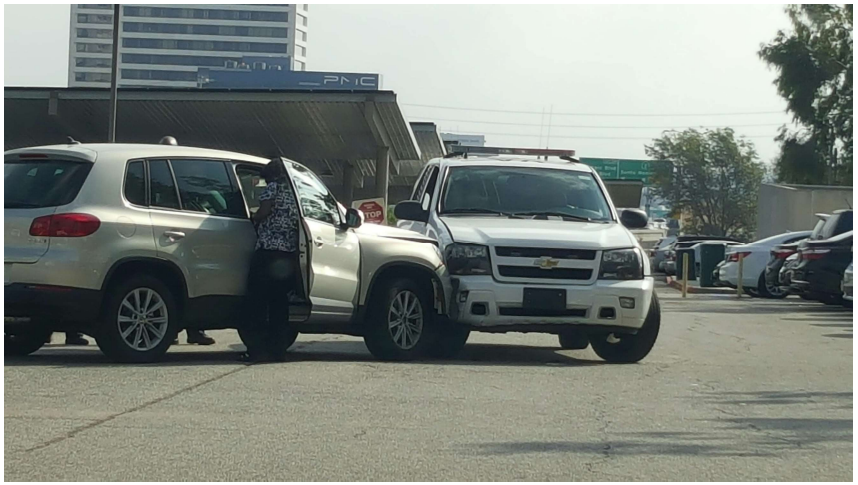
Apply for this position and are “hired” and sent a counterfeit check

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

FRIEND OR FAMILY IN TROUBLE

Triggering Incident, such as an accident

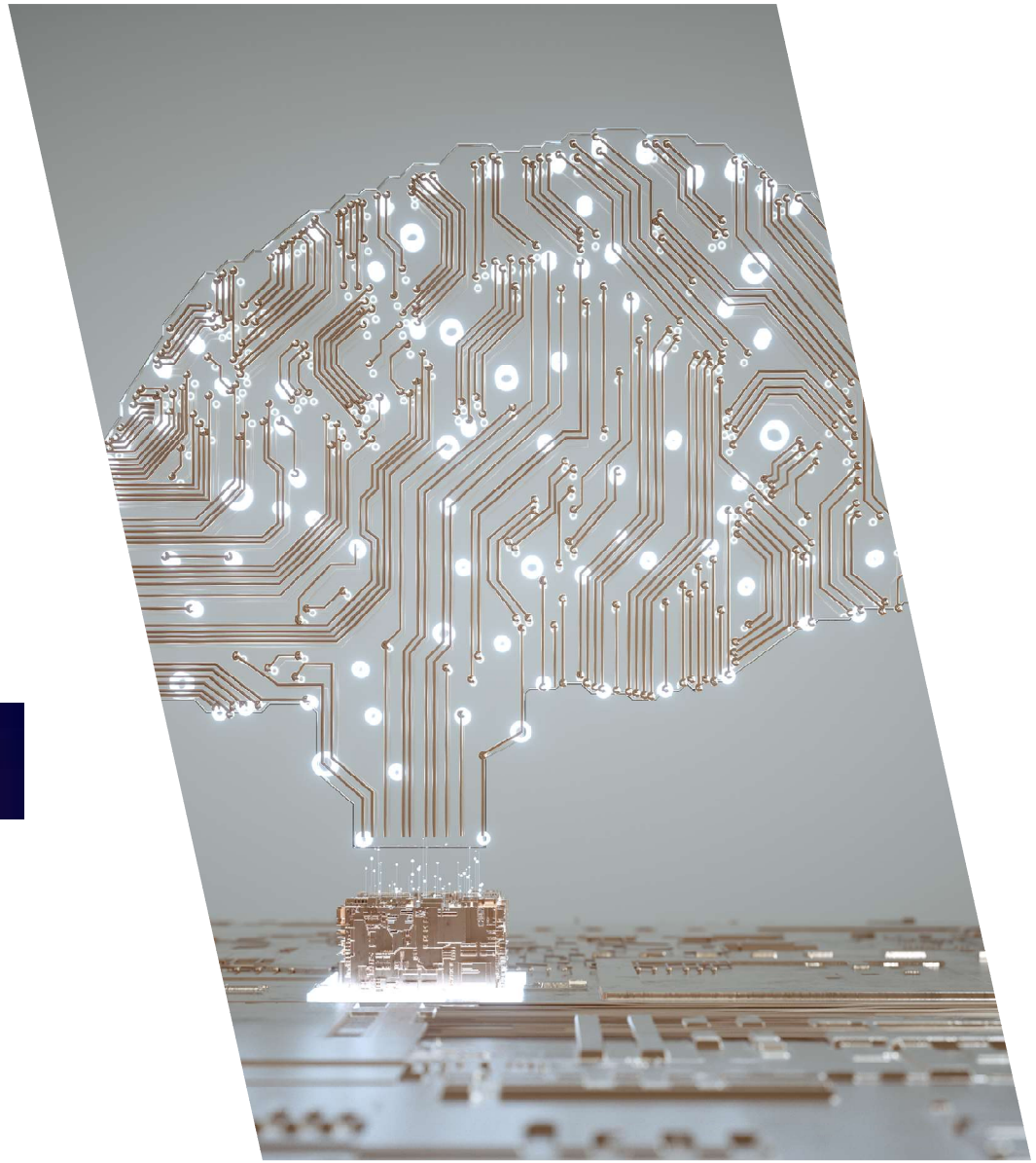
- Heightened Emotions
- Need to Act Quickly
- No Time to Reflect
- Isolation from Trusted Allies




BUDGET COINZ
BUDGET COINZ
bitcoin ATM
BUDGET COINZ

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.

HOW VOICE WORKS IN A DEEPFAKE

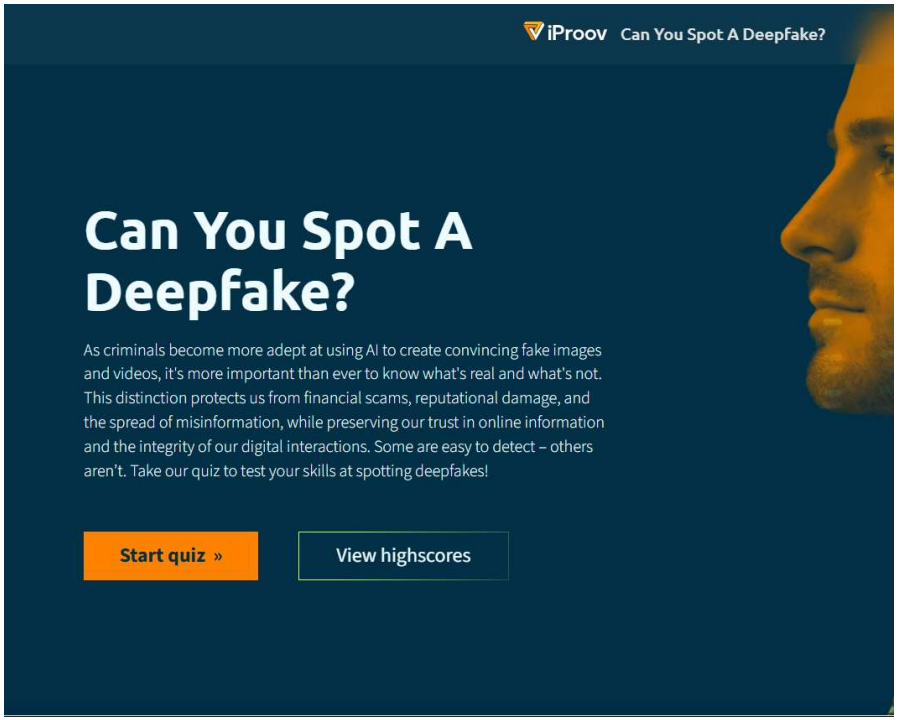
Only need 6 seconds of your voice

- 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

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/

CONVINCING VICTIMS

TRAUMA-INFORMED STRATEGIES

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

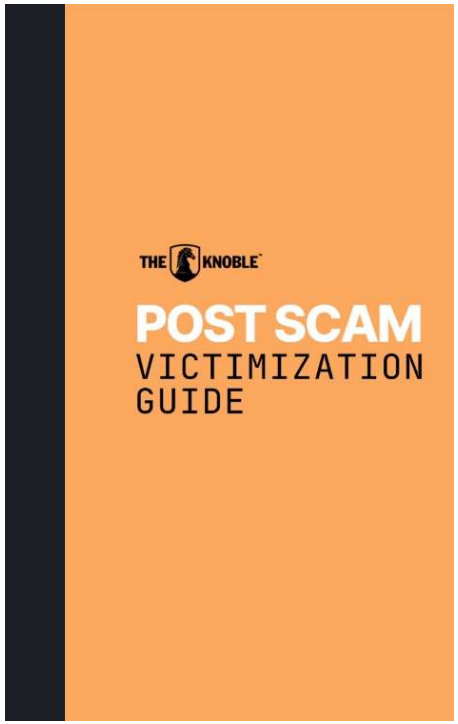
- Develop contact lists

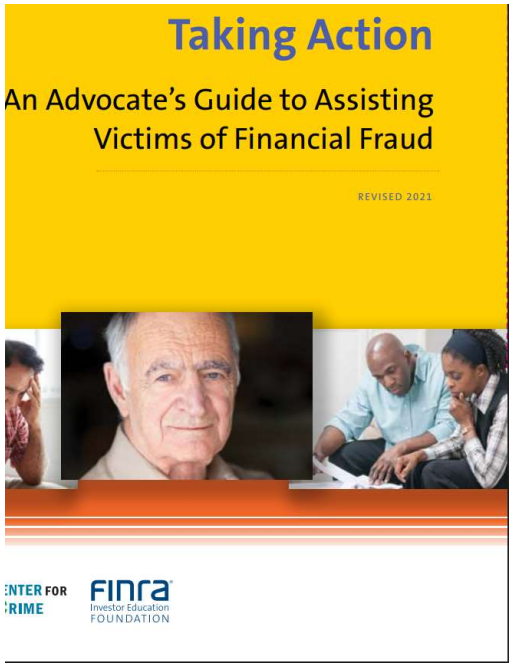
Training

- 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





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.

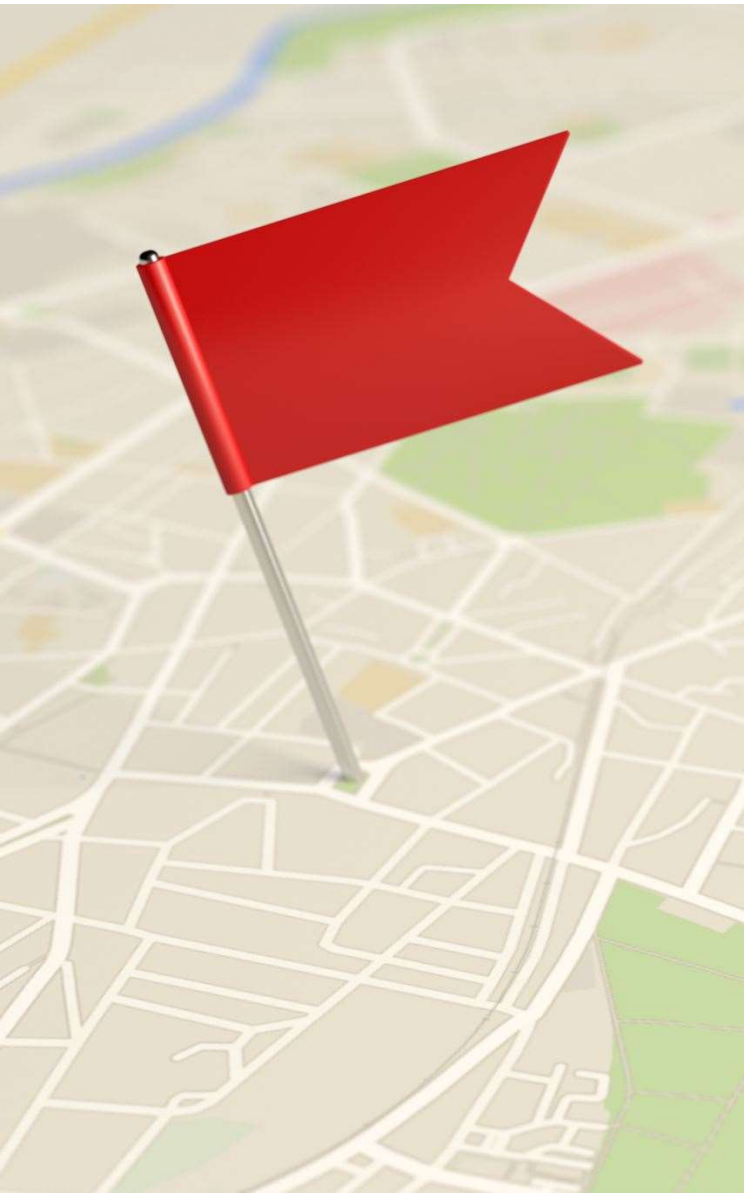
If you wish to send this wire, please contact me at the number below.

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
4. Contact joint accountholders or "trusted contacts"

BUILDING PARTNERSHIPS

- Develop policies on information sharing –GLBA exemption and State law
- Develop lists from existing cases
- ABA Fraud Directory: https://www.aba.com/banking-topics/risk-management/fraud/directory
- Join International Association of Financial Crimes Investigators: https://www.iafci.org/
- Join multidisciplinary teams, including https://theknoble.com/
- Obtain as much information as possible when reports are filed to facilitate law enforcement attention

NOTE: Assist victims in reporting, even if no or small loss amount



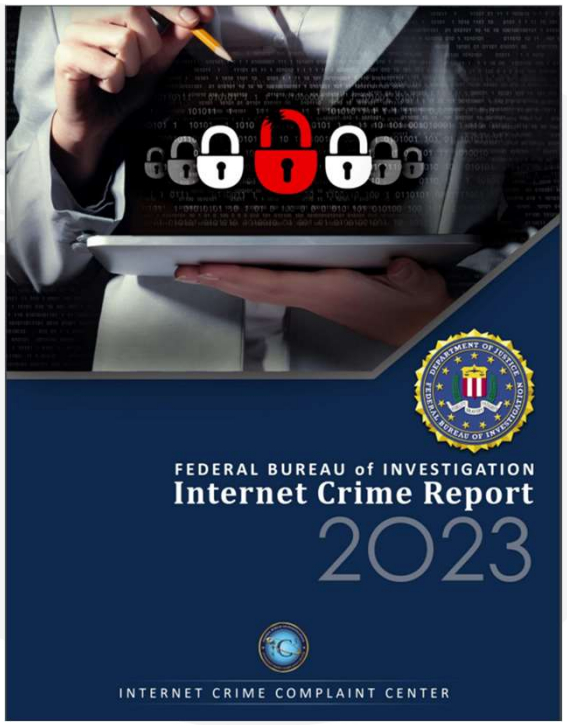
REPORT FRAUD TO LOCAL POLICE/ APS & FEDERAL GOVERNMENT AGENCIES

- 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

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") Ask: how did you receive it? • If mail, report to USPIS and contact our local reps to determine whether the address is a known fraud address. 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. • 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. Ask: Where are you taking the cash? · If Bitcoin ATM, report to the Secret Service. · If cash was mailed, report to USPIS. · 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: • Who are you sending the money to? • How did you meet the person who gave you the check/asked you to send a wire/Zelle/buy the gift cards? • Did they warn you not to tell the bank or say "it's a private matter"? • 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 1. Flag the account as Identity Theft and file a QAR with the details of the case. 2. Have the client visit the IDtheft.gov checklist. 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. 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.

SOLUTIONS

TECHNOLOGY SOLUTIONS TO COMBAT THE PROBLEM

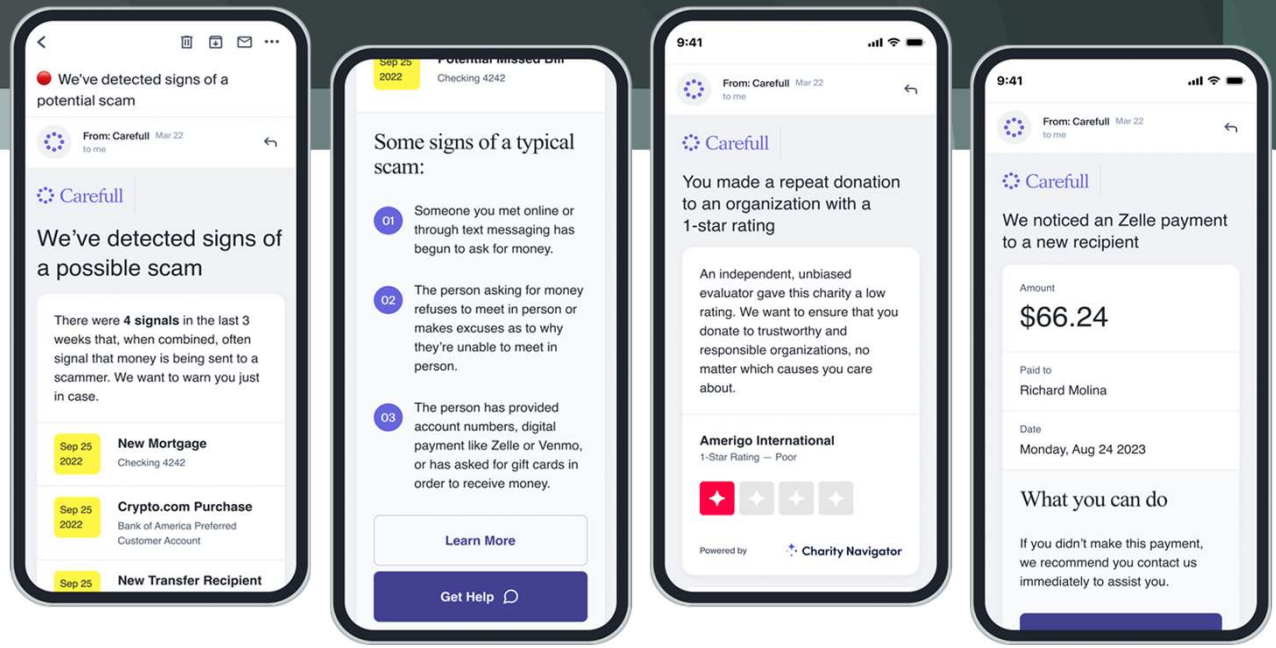
- Client solutions
- Report fraud online
- Identity verification
- Positive pay for checks and ACH
- Real-time transaction monitoring
- Fraud detection solution
- Artificial Intelligence / Machine Learning

AI/Machine Learning

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

Don't forget training for your staff /clients

Carefull



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	Zelle Crypto Gift Card Bill Change	Change of address, new account opened, stolen email, stolen

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

Laurel Sykes, EVP

Chief Risk Officer

American Riviera Bank

lsykes@arb.bank