AUXILIARY ORGANIZATIONS ASSOCIATION

THE NEXT ERA OF AUXILIARIES
SHAPING TOMORROW

Digital Deception

Staying ahead of fraud in an AI-powered world

PRESENTED BY
MIKE WATERCOTT & MALISA DAY
U.S. BANK

AOA GENERAL

Welcome to the era of synthetic reality

2026 AOA
ANNUAL CONFERENCE

What we'll cover

Fraud in the AI era: How modern tech fuels an already rampant fraud ecosystem

Payments fraud: Recent statistics in payment fraud

Fraud controls & best practices

Questions

Fraud in the AI era

2026 AOA
ANNUAL CONFERENCE

Collapse of trust

Why should we care about fraud?

Sophisticated fraud "ecosystem"

- Large degree of organization and specialization
- Sophistication and complexity
- Internal organizational support

Increase in complexity of fraud events

- Generative AI
- Social Engineering
- Credential compromise
- Mail theft (check fraud)
- Payment fraud (VEC)
- Ransomware / data breaches

Short- and long-term impacts

- Potential for significant loss
- Reputation risk
- Data and systemic impact
- Operational impact

Fraud is a risk, not an event

Wide spectrum of fraud

From low-tech
Mail Theft

To high-tech
Generative AI

2026 AOA
ANNUAL CONFERENCE

Source : https://www.fincen.gov/sites/default/files/shared/FinCEN%20Alert%20Mail%20Theft-Related%20Check%20Fraud%20FINAL%20508.pdf
Source: https://www.fincen.gov/sites/default/files/shared/FinCEN-Alert-DeepFakes-Alert508FINAL.pdf

What is Artificial Intelligence?

What is AI?

The theory and development of computer systems able to perform tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages.

What can it be used for?

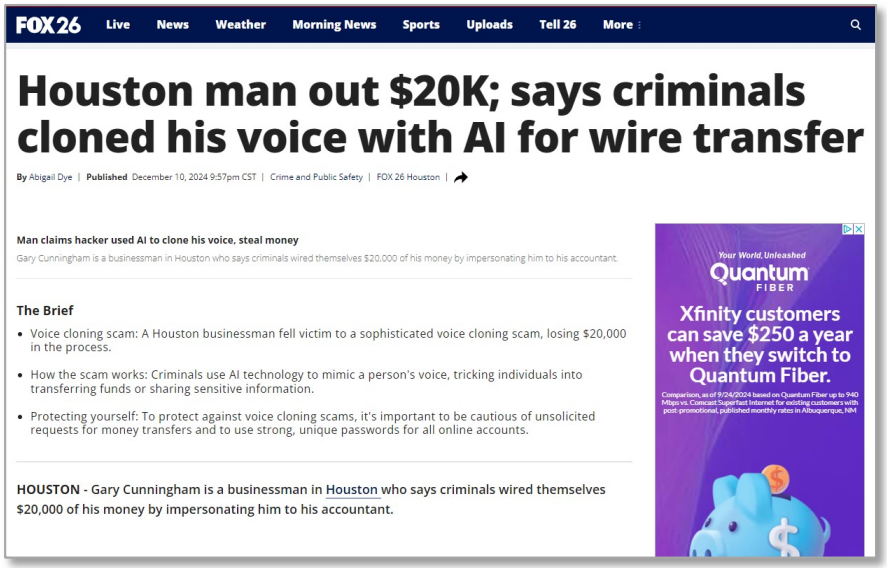
From self-driving cars to tools like ChatGPT, AI is transforming the way we live and work.

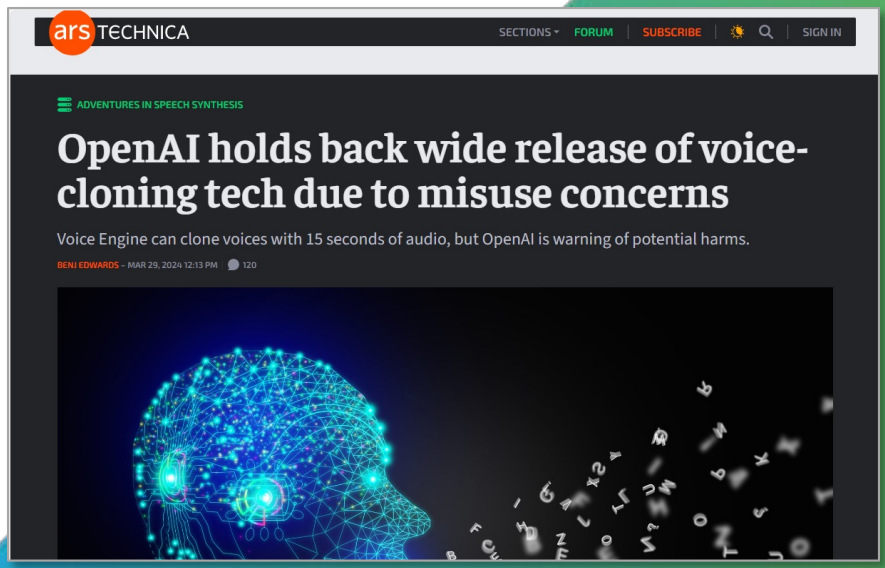
- AI generated text, images, audio (aka voice cloning), and video (aka deepfakes)

Source: FINCEN. Source: IC3.

The power of voice cloning

Scammers are starting to use the AI technology to commit crimes causing distressing situations for people all over the world. And in some cases, AI creators are holding off on the technology due potential misuse.





2026 AOA ANNUAL CONFERENCE

Source: Arstechnica. Source: FOX26.

Threat of AI-enhanced fraud

It’s real, and on the rise

ChatGPT has already been shown to be capable of generating
viruses, malware and phishing and social engineering campaigns

CNBC MARKETS BUSINESS INVESTING TECH POLITICS CNBC TV IN

TECHNOLOGY EXECUTIVE COUNCIL

A.I. is helping hackers make better phishing emails

PUBLISHED THU, JUN 8 2023•9:55 AM EDT

Bob Violino

SHARE

KEY POINTS

- Cyber criminals and other bad actors can do things faster and easier with artificial intelligence, which makes it more difficult for CISOs and other cybersecurity experts to protect their organizations.

Why Forcepoint Products Use Cases Resources

Home : Blogs : I built a Zero Day virus with undetectable exfiltration using only ChatGPT prompts

April 4, 2023 | 17 min read

I built a Zero Day virus with undetectable exfiltration using only ChatGPT prompts

Aaron Mulgrew

artificial intelligence

Deepfake payments fraud

In the headlines

World / Asia

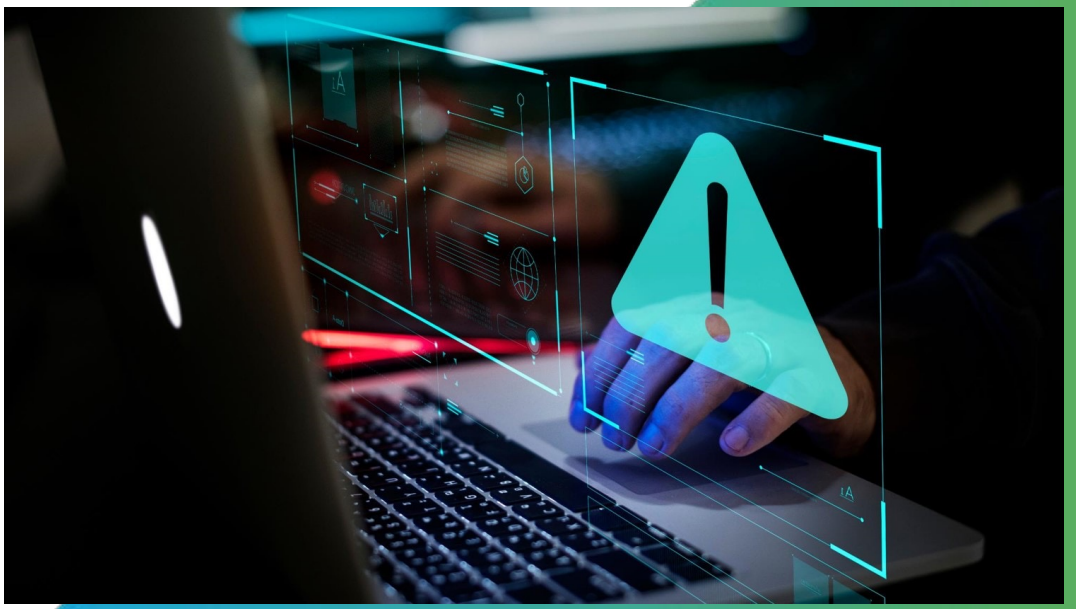
Finance worker pays out $25 million after video call with deepfake ‘chief financial officer’

By Heather Chen and Kathleen Magramo, CNN

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

Source: https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html

Payments fraud stats



2026 AOA
ANNUAL CONFERENCE

Top sources of fraud

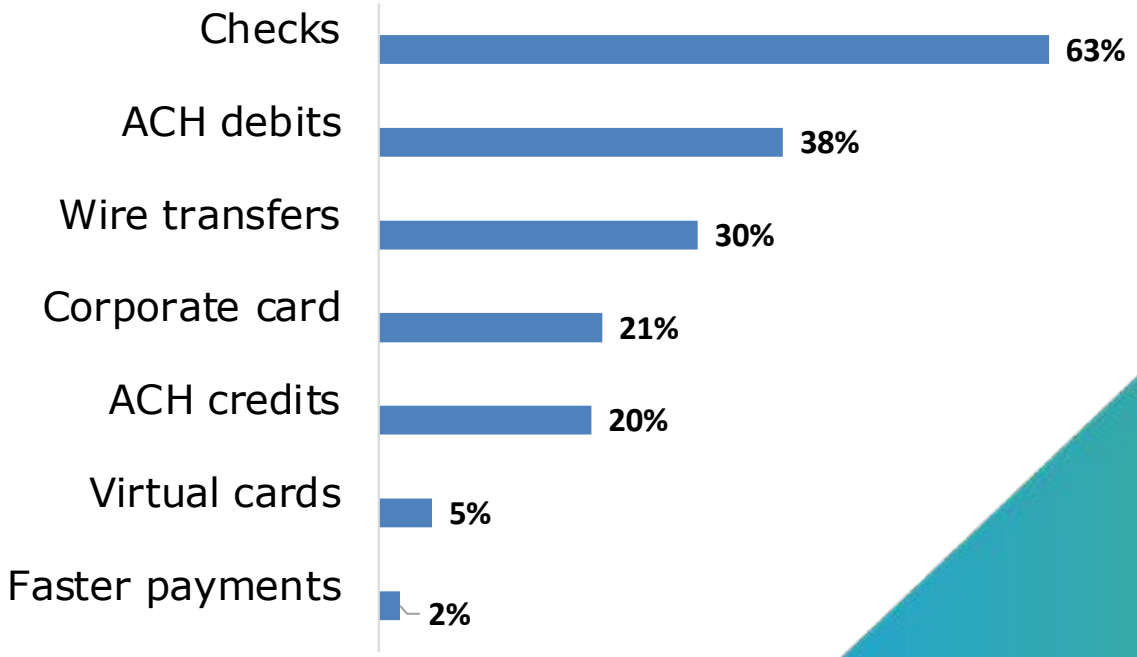
Percentage of organizations reporting attempted fraud

Business Email Compromise (BEC)	62%
Individual external to the organization using tactics other than email	49%
Vendor imposter	45%
Invoice fraud	24%
U.S. Postal Service office interference	23%
Imposter to a client posing as representative from your company	14%
Third-party or outsourcer (i.e. vendor, professional services provider, etc.)	12%
Account takeover (i.e. hacking a system, malicious code, etc.)	12%
Compromised mobile device due to spoof/spam text or call	8%
Organized crime ring (i.e. crime spree that targets multiple organizations)	7%
Deep-fake attempt (i.e. voice, vishing, etc.)	5%

Source: 2025 AFP® Payments Fraud and Control Survey Report
https://www.afponline.org/publications-data-tools/reports/survey-research-economic-data/Details/payments-fraud

Payment methods targeted

Percentage or organizations reporting attempted fraud



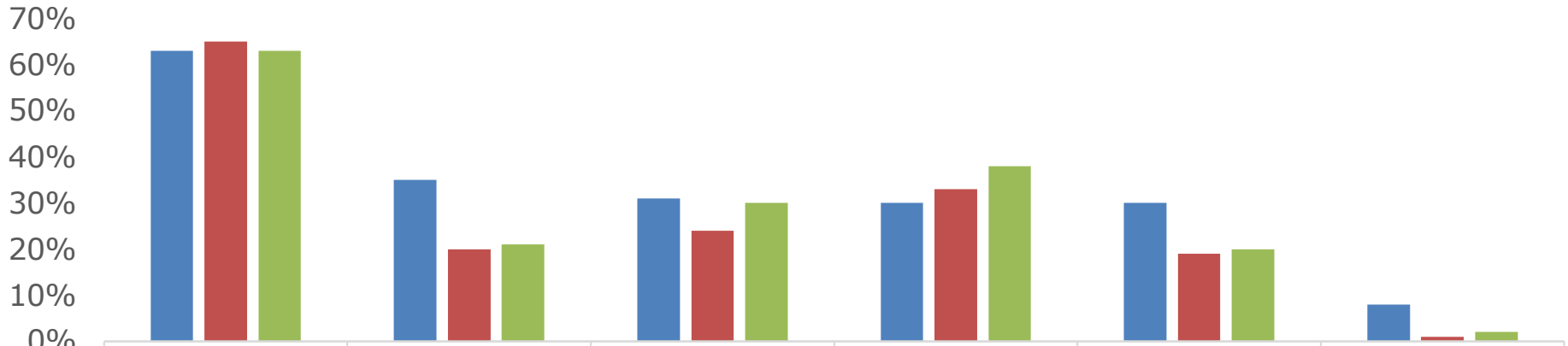
Checks and ACH continue to be the payment methods most impacted by fraud activity

2026 AOA ANNUAL CONFERENCE

Source: 2025 AFP® Payments Fraud and Control Survey Report
https://www.afponline.org/publications-data-tools/reports/survey-research-economic-data/Details/payments-fraud

3-year trends

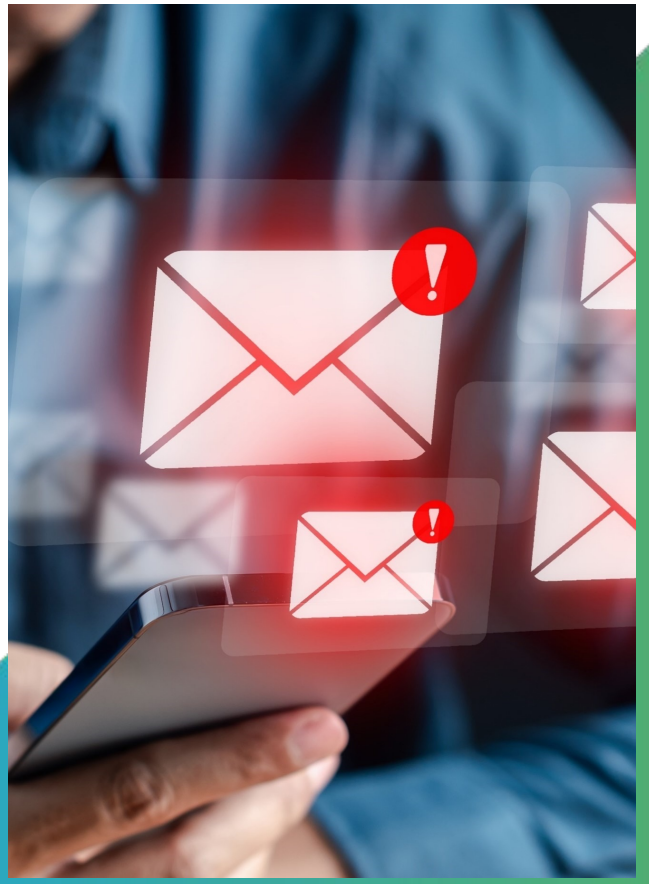
By payment type



	Check	Corporate credit card	Wire	ACH debit	ACH credit	Faster payments
2022	63%	35%	31%	30%	30%	8%
2023	65%	20%	24%	33%	19%	1%
2024	63%	21%	30%	38%	20%	2%

Source: 2024 AFP® Payments Fraud and Control Survey Report
https://www.afponline.org/publications-data-tools/reports/survey-research-economic-data/Details/payments-fraud

Fraud in your inbox



2026 AOA
ANNUAL CONFERENCE

Email compromise

Continues to grow and evolve

Email compromise is a type of cybercrime where attackers use various tactics, such as phishing and malware, to gain access to victims' email accounts. Once access is secured, attackers trick or threaten the target to make a fraudulent financial payment. Email compromise can include:

- Business Email Compromise (BEC)
- Email Account Compromise (EAC)
- Vendor Email Compromise (VEC)

21.4K

Complaints in 2024

$2.7B

Adjusted losses in 2024

Source: https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

Email compromise variants

Business Email Compromise (BEC)	Email Account Compromise (EAC)	Vendor Email Compromise (VEC)
Impacts targeted organization and employee. Victim is typically employee following fraudulent payment instructions.	Impacts organizations and individuals (email owner and contacts) and can range from financial loss to data exposure.	A scam where the fraudster impersonates a 'trusted' vendor/partner for financial gain. Impacts go beyond organization to affect clients and customers with potential financial loss and malware deployment.

Vendor email compromise

The difference between BEC and VEC

While traditional BEC attacks usually claim to be from a trusted individual within the organization, VEC goes one step further: it impersonates vendors (or other trusted third parties) to trick the target into paying fraudulent invoices, disclosing sensitive data or granting access to corporate networks and systems.

Research

Cyber actor conducts open-source research on awarded and ongoing projects and companies.

Domain registration

Cyber actor creates a spoofed domain like the legitimate company.

Business Email Compromise (BEC)

Cyber actor sends an email to a customer of the legitimate company requesting a change to payment information.

Information change

Customer believes the email is legitimate and changes banking information.

Transfer

Customer transfers money to new account and the cyber actor receives the money.

Fraud controls

2026 AOA
ANNUAL CONFERENCE

Payment fraud mitigation

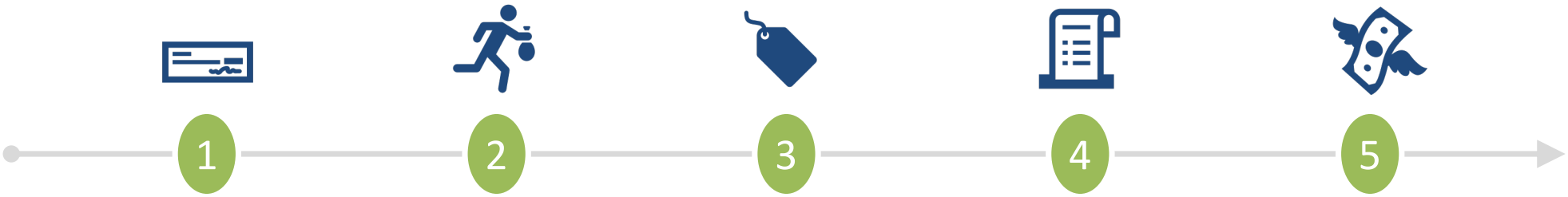
Validate

Validate

Validate

…Only then send.

Stolen check lifecycle



1. Client creates and mails check
2. Check is stolen from the mail
3. Check is posted for sale online
4. Check is purchased by threat actor
5. Threat actor attempts to obtain funds

Fraud Threat Disruption team intervention methods

1. Locates compromised item
2. Researches and attempts to identify impacted customer
3. Performs outreach to branch, RM's and Ops as needed
4. Bank performs outreach to customer
5. Bank works with customer to take any necessary action

Standard fraud intervention methods (holds, escalations)

Best practices

To avoid check fraud

Types of check fraud

- Check kiting
- Embezzlement
- Abandonment
- Forgery

Types of fraud control strategies

- Payee Positive Pay
- Daily account review and recon
- Segregation of accounts
- Tamper resistant check features
- Use electronic alternatives!

Source: AFP® 2025 Payments Fraud & Control Report.

Validation tools

Confirm the destination of electronic payments

Before you pay

In addition to independent callbacks…

- Confirm account status and ownership

Rely on a trusted source

Account validation, via Early Warning, connects you to a secure national shared database of checking and savings accounts formed by thousands of trusted financial institutions as your source for verification.

Be aware and be skeptical

Especially in the era of Artificial Intelligence

Use a secret word	Never share sensitive information	Do not send money or gifts	Listen closely to voices
Create a secret word or phrase with your family to verify their identity.	Never share sensitive information with people you have met only online or over the phone.	Do not send money, gift cards, cryptocurrency, or other assets to people you do not know.	Listen closely to the tone and word choice to distinguish between a legitimate caller and an AI-generated one.

Subtle imperfections	Limit online content	Verify caller's identity
Look for subtle imperfections in images and videos, such as distorted hands or feet, unrealistic teeth or eyes, indistinct or irregular faces.	If possible, limit online content of your image or voice, make social media accounts private, and limit followers to people you know.	Verify the identity of the person calling you by hanging up the phone, researching the contact of the bank or organization purporting to call you, and call the phone number directly.

Source: IC3

Fraud prevention best practices

Ensure your banking partners have experience in dealing with payments fraud

- Prioritize digital payment methods
- Incorporate a multi-layered process on significant transactions
- Train (and test) employees
- Automate high-risk tasks (i.e. outsource checks, partners to onboard / screen vendors)
- Incorporate a regular fraud checkup with your bank to identify gaps in protection
- Understand timing to action exceptions
- Set defaults to not pay if deadlines are missed

Act immediately

Have a plan for your fraud response

Contact your financial institution immediately, and request to open a fraud case

Contact your local FBI Office and file a complaint

Also file a complaint with the FBI's Internet Crime Complaint Center (IC3)

2026 AOA ANNUAL CONFERENCE

Source: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf.

AUXILIARY ORGANIZATIONS ASSOCIATION

THE NEXT ERA OF AUXILIARIES
SHAPING TOMORROW

THANK YOU!