American Bankers Association

Building Success. Together.

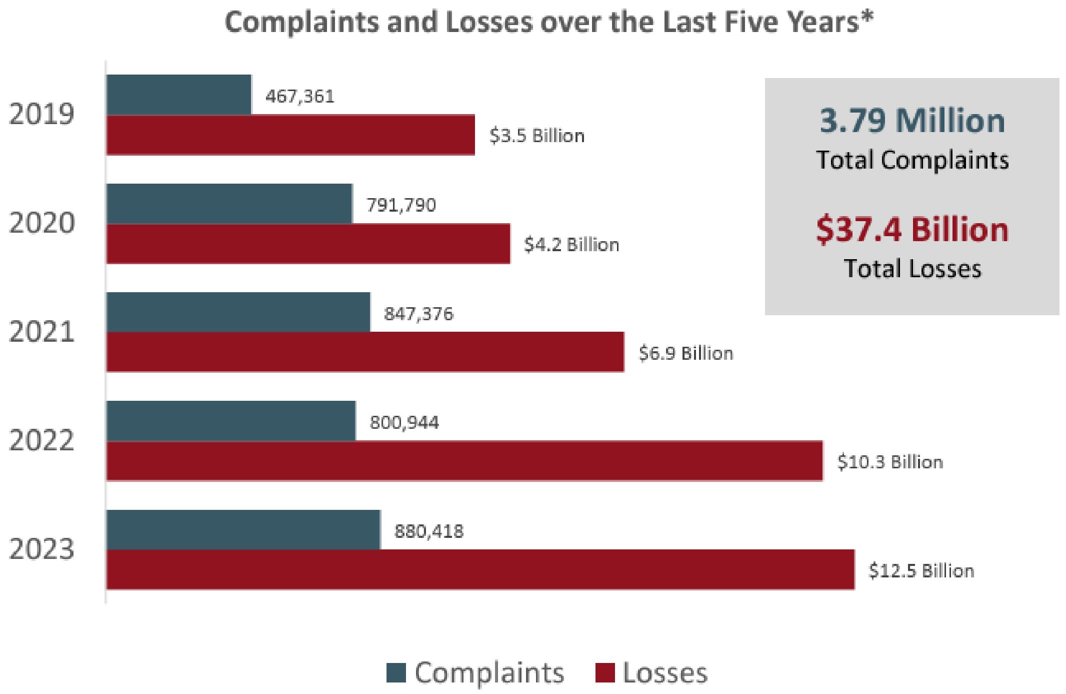
Consumer Fraud Risks
Agenda Items

1. State of Fraud – A statistical analysis
2. Social Engineering
3. Check Fraud
4. AI Risks
5. Questions

2024 Fraud Statistics

- Social Engineering scams were **10 times** more dominant from 2023 to 2024 in North American financial institutions. *BioCatch, 2024 Digital Banking Fraud Trends*.
- Check fraud **tripled**. *BioCatch, 2024 Digital Banking Fraud Trends*
- Stolen data surged driven by the theft of **269 million card records and 1.9 million checks**. *Alloy, 2024 Financial Fraud Statistics*.
- **50%** of banks, fintechs and credit unions reported an increase in business fraud, and **2/3rds** reported an increase in consumer fraud. *Alloy, 2024 Financial Fraud Statistics.*

FBI IC3 – 2023 Internet Crime Report



- Identity Theft
  - 2020 – 43,330
  - 2021 – 51,629
  - 2022 – 27,922
  - 2023 – 19,778
- 2022 – 46% drop in ID theft claims
- 2024 National Public Data Breach – 2.9B personal records

FinCEN Jan 2024 Financial Trend Analysis

Figure 2. Top Typologies Reported, January to December 2021[36]

Typology	Number of BSA reports	Total Suspicious Amounts
General Fraud	1.2 million	$149 billion
False Records	~423,000	$45 billion
Identity Theft	~222,000	$36 billion
Third-Party Money Laundering	~154,000	$18 billion
Circumventing Standards	~110,000	$12 billion
Total	**2.1 million**	**$260 billion**

- Some of the best estimates of total fraud can come from SARs
- TOTAL Identity Related SARS Filed - **$351 Billion**

https://www.fincen.gov/sites/default/files/shared/FTA_Identity_Final508.pdf

FRAUD AS A SERVICE

Fraud as a Service (FaaS) represents a evolution in the world of cybercrime, where illicit services and tools are offered on a subscription or pay-per-use basis.

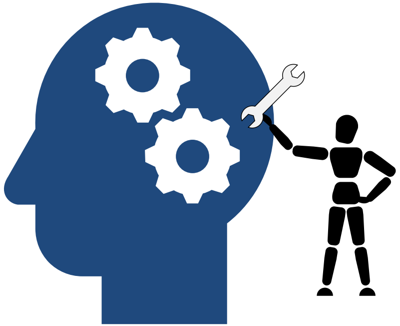
The service replaces the need for the criminal's sophisticated technical expertise with packaged fraud tools and schemes.

This offers, among other fraud tools:

1. fake identities
2. hacking tools
3. bespoke phishing campaigns and
4. malware

Social Engineering

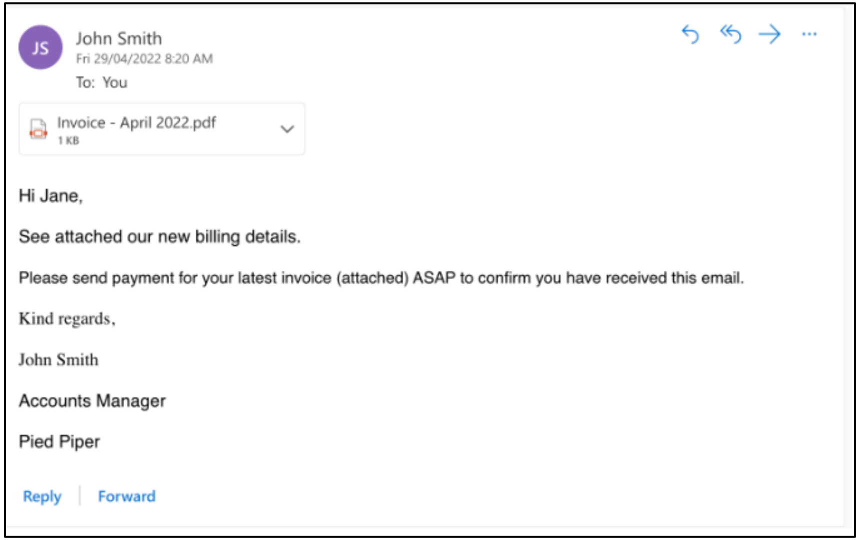
Social Engineering



- Taking advantage of trust
  - Phishing – Doubled in 2024
  - Text and phone number spoofing
- Attacking the customer
  - As Banks have improved their detection of false emails, phone calls and identity, criminals have moved their focus to the customer
  - Customer centric attacks begin outside of bank controls, often making banks the last point of the compromise.

Business Email Compromise

- Low effort – Large rewards
  - Ubiquiti, a networking company, received false vendor email requests to transfer funds overseas for over $46 Million in losses.
  - Facebook and Google receive false vendor invoices for over $120 Million in loses.
  - St. Ambrose Church received false vendor emails from its construction company informing the church it had changed its bank account. This let criminals take $1.75 Million from the church.



JS John Smith
Fri 29/04/2022 8:20 AM
To: You

Invoice - April 2022.pdf
1 KB

Hi Jane,

See attached our new billing details.

Please send payment for your latest invoice (attached) ASAP to confirm you have received this email.

Kind regards,

John Smith

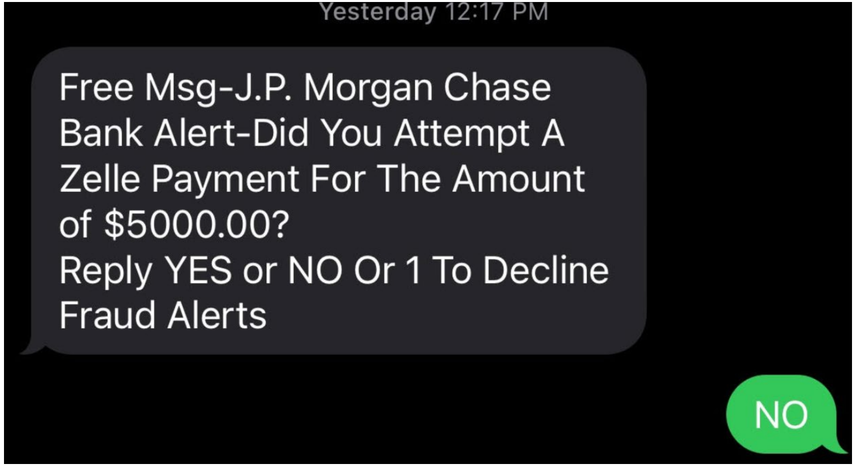
Accounts Manager

Pied Piper

Reply | Forward

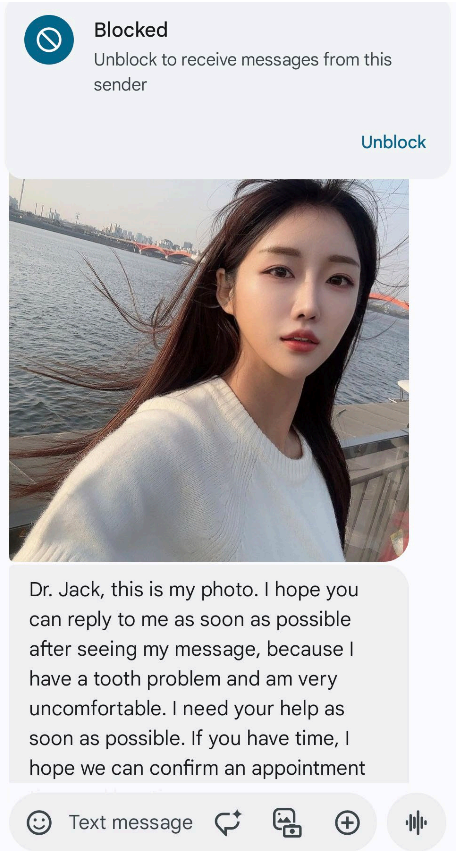
UpGuard.com

Text Fraud – Shifting to Bank Impersonation



- FTC stated number text scam – bank impersonation
- Original focus on convincing P2P payments
- Fraudster socializes username and initiates password change
  - To defeat 2 step auth, fraudster keeps victim on phone and gets passcode to change password
- Now using fraud alerts to try and get funds out of accounts

Texts – Starting Point for Romance or Crypto Investment Schemes



2023 CRIME TYPES WITH CRYPTOCURRENCY NEXUS *Continued*

LOSSES

Crime Type	Loss	Crime Type	Loss
Investment	$3,961,033,779	Phishing/Spoofing	$9,630,206
Personal Data Breach	$494,493,759	Extortion	$9,281,906
Tech Support	$420,904,388	BEC	$4,768,674
Confidence/Romance	$215,821,314	Lottery/Sweepstakes/Inheritance	$4,462,513
Data Breach	$150,154,167	Credit Card/Check Fraud	$3,317,381
Government Impersonation	$112,878,842	Identity Theft	$2,732,795
Advanced Fee	$39,375,337	Harassment/Stalking	$1,854,329
SIM Swap	$30,263,667	Overpayment	$1,582,857
Ransomware*	$27,355,793	Real Estate	$887,285
Other	$26,258,782	Malware	$341,178
Non-payment/Non-Delivery	$19,656,091	Crimes Against Children	$185,921
Botnet	$17,002,000	IPR/Copyright and Counterfeit	$51,952
Employment	$10,104,795	Threats of Violence	$27,500

FBI IC3 Crypto Complaints

- 2020 ~ $500M
- 2021 ~ $1.5B
- 2022 ~ $3.75B
- 2023 ~ $5.6B

HOW TO MANAGE THE RISK

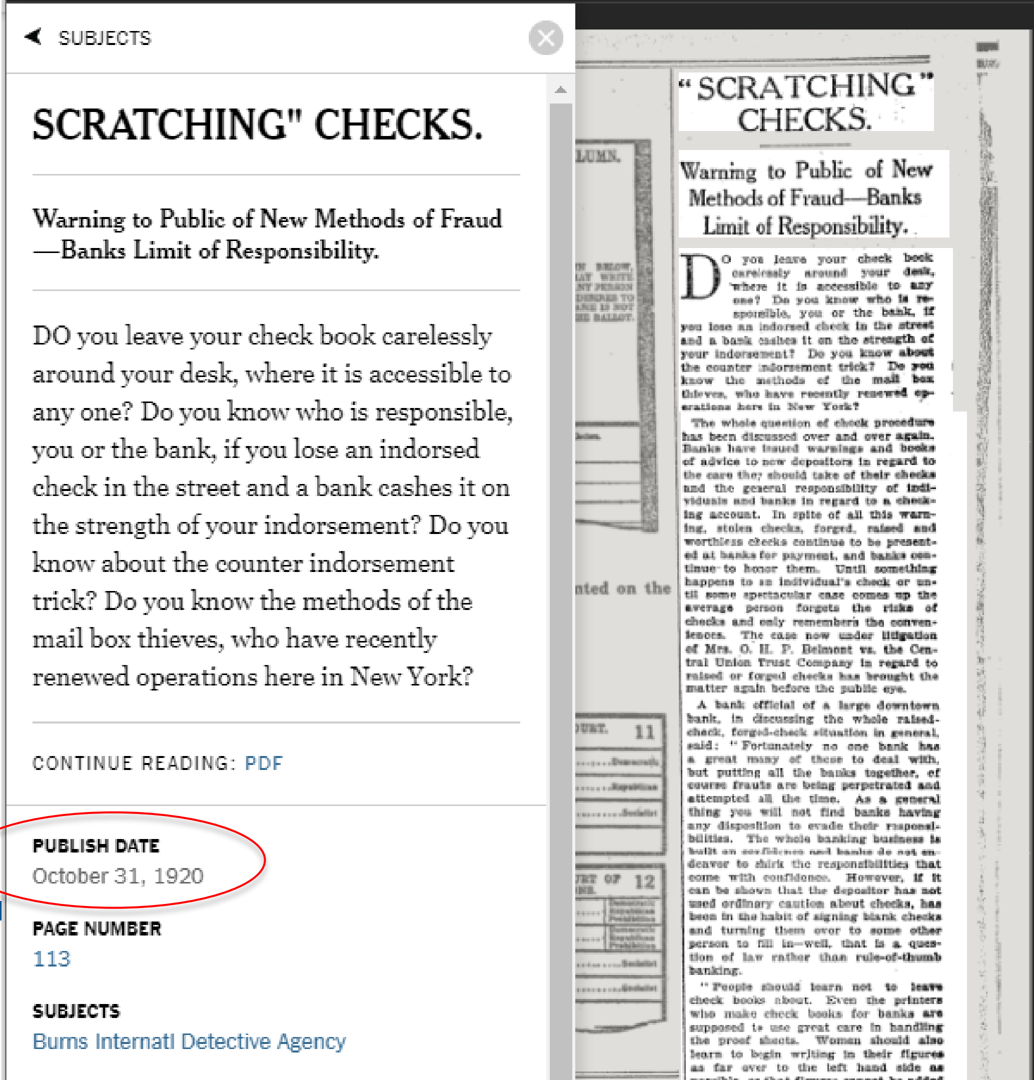
- Client education.
  - Establish warnings in your texts, on your online portal and on your webpage to educate clients about schemes.
  - Provide your client facing staff with talking points to navigate conversations about the risks of social engineering
  - Consider hosting client events on the risks of social engineering
- Processes and System controls
  - Establish staff training on when to reject a transfer request or escalate to close an account
  - Train your systems for patterns of social engineering (new login locations, small test transfers, etc.)

Check Fraud

Check Fraud

From NYT 1920

> "Do you know the methods of the mailbox thieves who have recently renewed operations here in New York?"



SUBJECTS

SCRATCHING" CHECKS.

Warning to Public of New Methods of Fraud —Banks Limit of Responsibility.

DO you leave your check book carelessly around your desk, where it is accessible to any one? Do you know who is responsible, you or the bank, if you lose an indorsed check in the street and a bank cashes it on the strength of your indorsement? Do you know about the counter indorsement trick? Do you know the methods of the mail box thieves, who have recently renewed operations here in New York?

CONTINUE READING: PDF

PUBLISH DATE
October 31, 1920

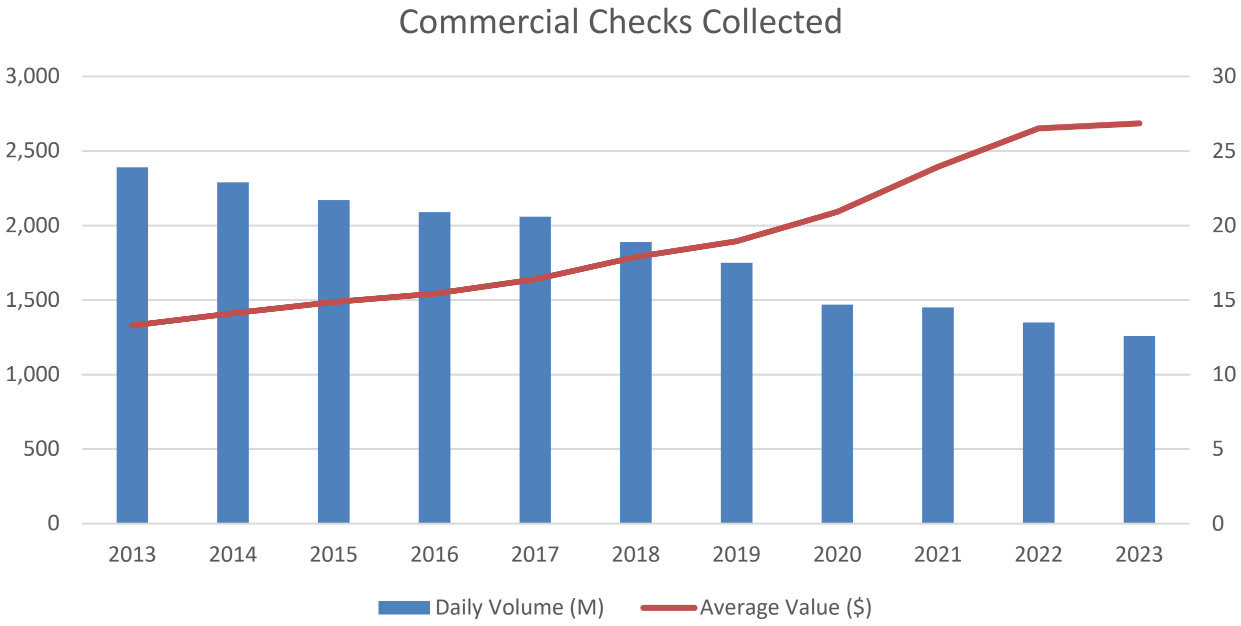
PAGE NUMBER
113

SUBJECTS
Burns Internatl Detective Agency

"SCRATCHING" CHECKS.

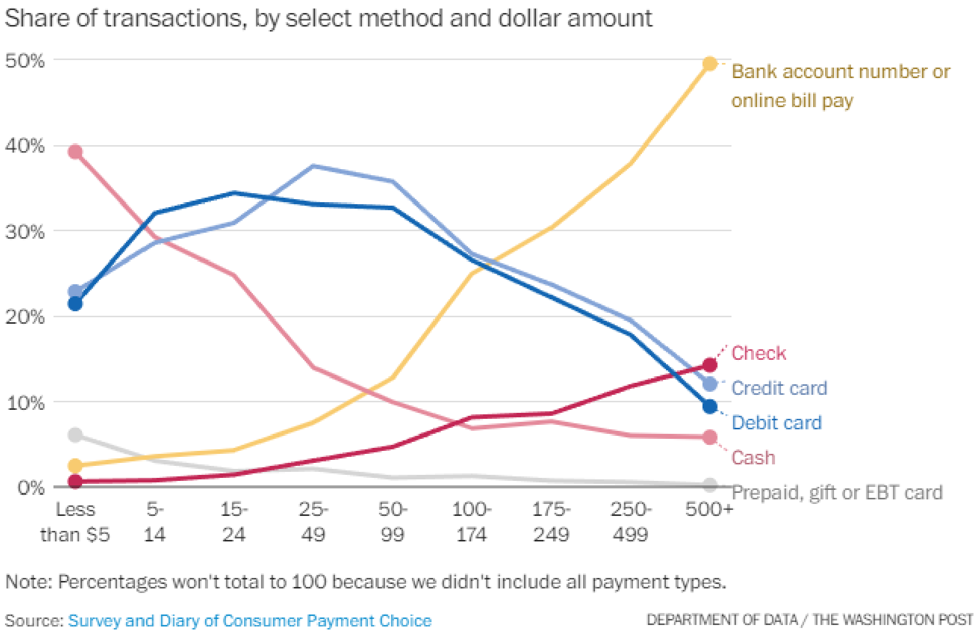
Warning to Public of New Methods of Fraud—Banks Limit of Responsibility.

People Still use Checks – but less



https://www.federalreserve.gov/paymentsystems/check_commcheckcolannual.htm

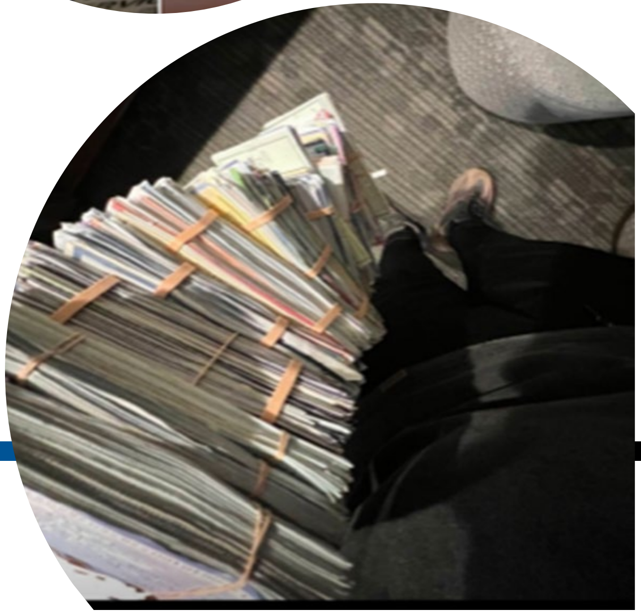
People Still use Checks – for higher dollar purchases



ACTIVE	DESCRIPTION	CHECK
Contractors	Building contractors, plumbers, electricians, HVAC	43
Charity	Charitable or religious donations	35
Government	Government taxes or fees	27
Rent	Rent for apartments or homes	19
Utilities	Electricity, water, sewer, trash	14
Health care	Hospital, doctor, dentist, nursing home	12
Education	Schools, colleges, child care centers	11
Professionals	Lawyers, accountants, architects, veterinarians, photographers	11
Personal	Gifts and repayments to family or friends	9

Source: Survey and Diary of Consumer Payment Choice

Check Fraud



- Check fraud accounted for **66% of payment fraud**, followed by 37% for ACH debit fraud.
- 2023 Check fraud increased over **180% from 2022.**
- Losses totaled $24 billion in United States.
- The primary source of check fraud is the **United States Postal System,** compromised by fraud gangs and their theft of **Arrow Keys**.
- Common examples of arrow keys for an entire zip codes available for **sale for ~$4000.**
- High volume mail theft increase over 139% the last 4 years.

Mail Theft Evolution

USA Today
https://www.usatoday.com › money › 2023/07/05 › us...
U.S. Postal Service theft, mail carrier robberies on rise. ...
Jul 5, 2023 — Should you be concerned about mail **theft**? · Glue traps: **Thieves** use a sticky substance on the door of the **mail box** to catch mail, which they can ...

CBS News
https://www.cbsnews.com › MoneyWatch
Avoid mailing your checks, experts warn. Here's what's ...
Jun 22, 2023 — Mail **theft** and fraud are on the rise, with **thieves** breaking into USPS **mailboxes**, stealing checks from homes and robbing mail carriers.

abc11.com
https://abc11.com › mail-theft-postal-carriers-check-w...
Thieves target postal carriers, mail drop-offs in attempt to steal ...
Dec 15, 2022 — Maimon said thieves are getting the stolen checks by either swiping ... in mail theft incidents -- such as **mailbox thefts** and postal carrier ...

Check Fraud Statistics

- **$2430 is average** amount of fraudulent check
- **50%** of fraudulent checks **> than $500**
- Less than 10% are **> $5000**
- **75%** of fraudulent checks are on **business accounts**
- Less than 10% are remotely created
- The volume of check fraud has **stressed the banking system** and warranty breach claims are being **significantly delayed.**

- Average volumes vary significantly between banks from 500 to 30,000 per month.
- The challenges are **backlogs** in check warranty claims, Availability of Funds and larger check values.
- This impacts the **speed of claims**: processing varies from 10 to 90 days.
- The impact is also being felt on **overhead** costs with banks reporting 30% + increase in staffing levels.
- For every **$1 of a fraudulent transactions** attempted **FIs incur $4.36 in costs.**

ABA Fraud Contact Directory

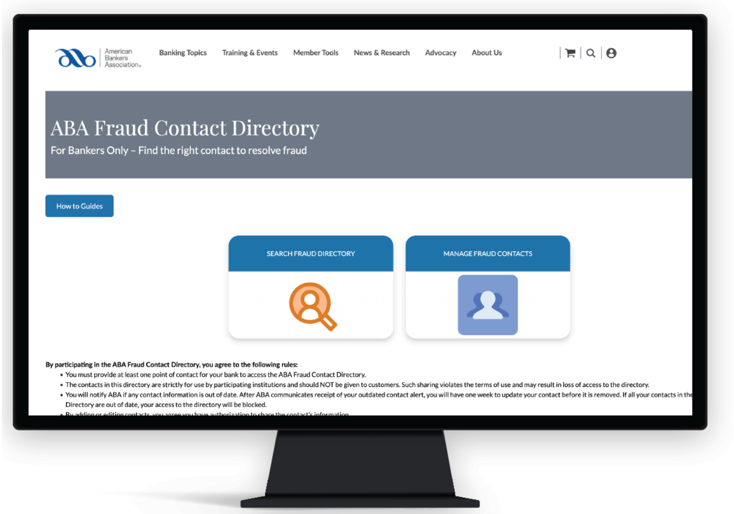
The coordination of fraud efforts between banks requires a designated point of contact for submitting claims or requests. The ABA Fraud Contact Directory, originally the ABA Check Fraud Claim Directory, helps participants find the appropriate contact for ACH, Wire, FedNow, TCH RTP, and Check Fraud.

Positive feedback from participants:

"We are all so excited to spend less time on the phone with different FIs trying to get to the right department or trying to get them to supply their information"

"I wanted to share with you how valuable the ABA Check Fraud Claim Directory has become…Prior to the creation of the directory, we would have been in an endless loop of being pointed to different departments."

"ABA Fraud Directory… is usually where I find all the banks I am searching for."



Manage Fraud Contacts

Banks can add, edit, and remove fraud contacts for their affiliated institutions.

They also have the ability to upload claim requirements for their organization.

Report Outdated Contacts

Any bank can report outdated contacts for other institutions. If a bank has only an inactive email address listed, their access to the directory will be suspended.

Search Fraud Directory

Search for participating banks using their FDIC number or bank name to find the appropriate contact.

To access the search feature, banks must provide at least one fraud contact.

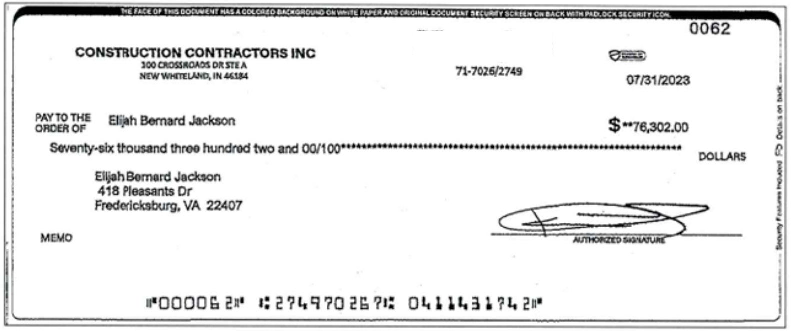
ABA Check Fraud Toolkit

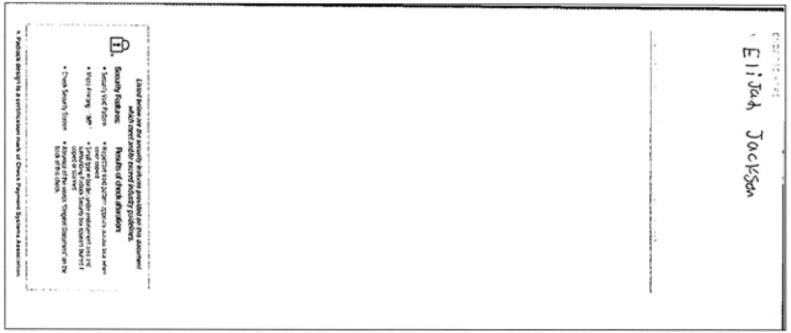
Claim Type Definitions

- Altered Check Claim
- Indorsement Forged / Incorrect
- Missing Indorsement
- Unauthorized Remotely Created Checks
- Counterfeit Check
- Forged or Unauthorized Maker Signature Claims
- Subject to Midnight Deadline
    - Counterfeit Check
    - Forged or Unauthorized Maker Signature Claims

Messaging: Protecting Customers and Banks

- Customer messaging
  - Minimize use of checks
  - Move toward electronic payments/payroll
  - Enroll in Payee Positive Pay
  - Do not use blue mailboxes
  - Watch accounts closely
- Banks
  - Require use of positive pay or have customer sign indemnification agreement
  - Relook Deposit Agreement T&Cs
  - Ask core to review check fraud capabilities
  - Relook funds availability for all channels
  - Review all check transactions the day they arrive

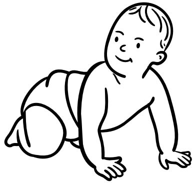




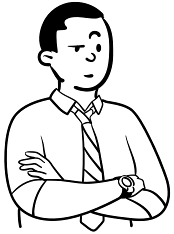
Artificial Intelligence

Artificial Intelligence and the Fraud Nexus

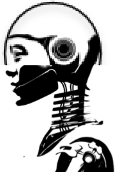
- Evolution of Protection and Attacks
  - Rule Based
    - Each instance is reviewed by a rule to provide an action
      - No memory of prior rule results
      - Transaction based



  - Machine Learning
    - Each instance is reviewed by a rule or rules, and compared to prior rule results
      - Limited to the scope of the product
      - Category based



  - Artificial Intelligence
    - Each instance is reviewed by a rule or rules. Logic is applied to the transaction based on prior attempts, outside data and predictive analysis.
      - Requires a learning curve
      - Can be applied to account level



The use of AI brings benefits and risks

Potential Benefits

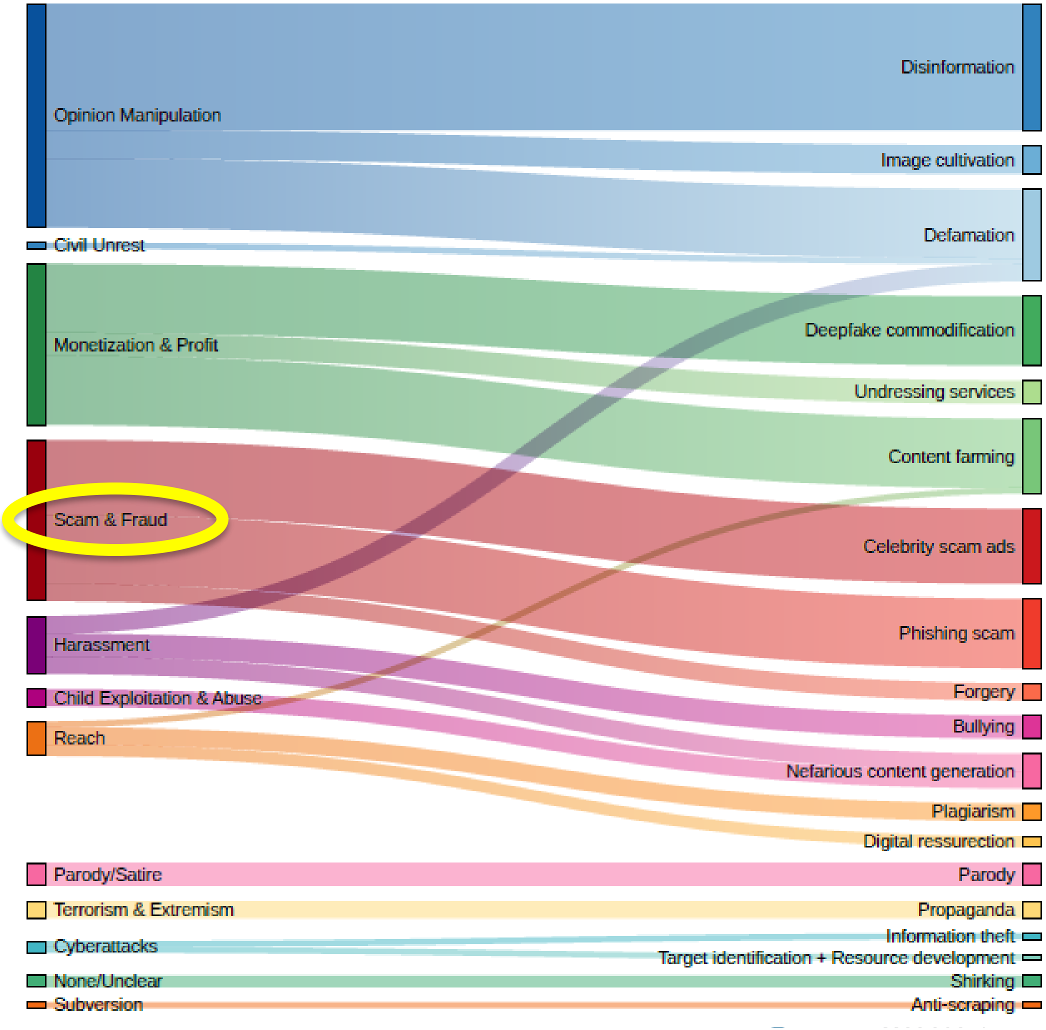
- Generate unique insights
- Automate activities
- Reduce human error
- Eliminate repetitive tasks
- Accelerate results

Potential Risks

- Transparency and exploitability
- Algorithmic bias
- Use by bad actors
- Deep fake confusion
- Copyright issues in training data
- Privacy

GenAI Misuse

- Google DeepMind Division
- Most common goal was "influence public opinion, enable scam or fraudulent activities, or to generate profit"
- "predominantly seeing an exploitation of easily accessible GenAI capabilities requiring minimal technical expertise"
- Analyzed incidents from Jan 2023 to Mar 2024 from different social media platforms



https://arxiv.org/abs/2406.13843

Fraud Uses of AI

- Phishing and Spear Phishing
- Password Compromises
- Biometric Compromises
- DeepFake

- AI does not necessarily create new fraud techniques. It increases the speed and efficiency of the traditional fraud.

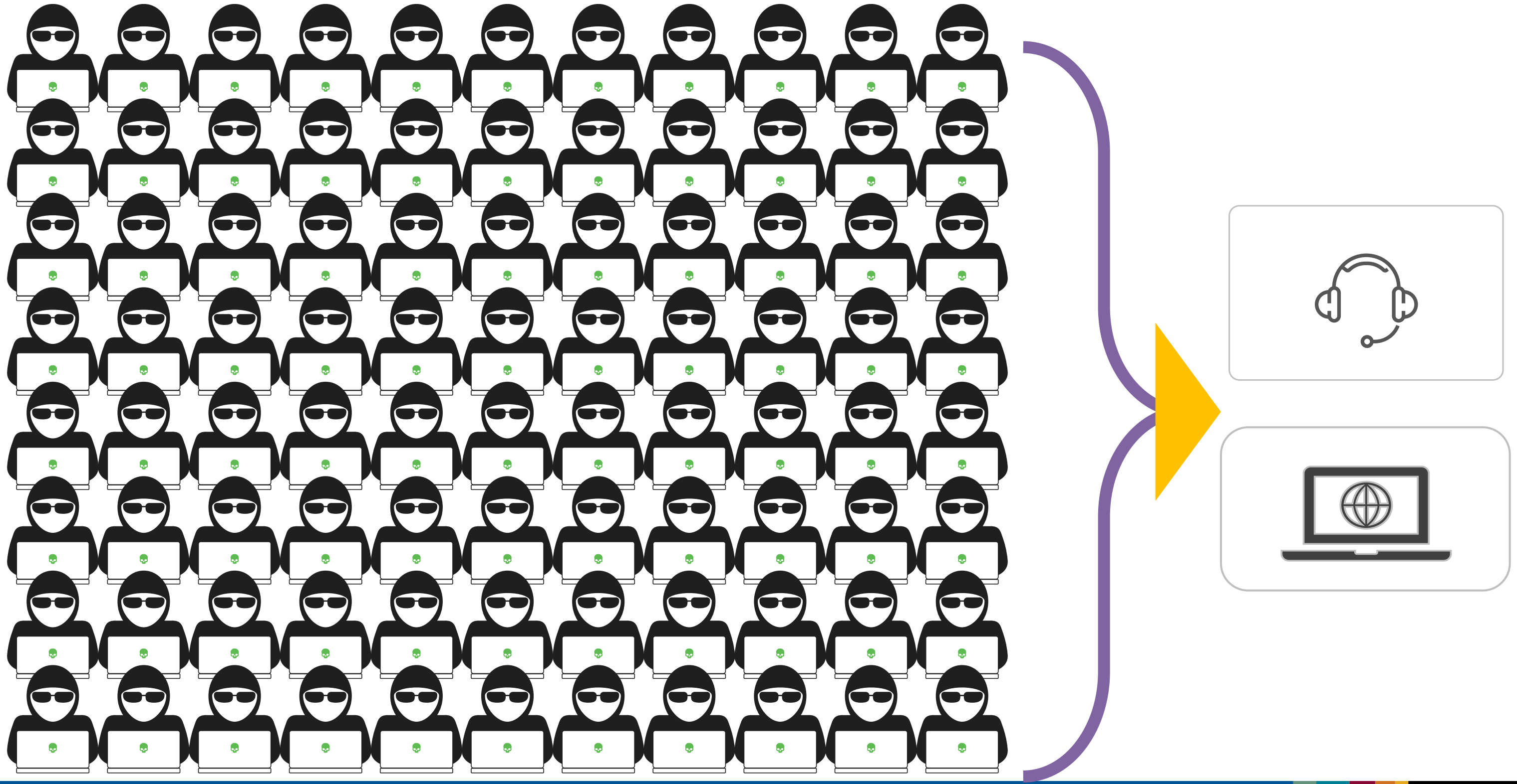
WHICH IS FAKE?

WHICH IS FAKE?

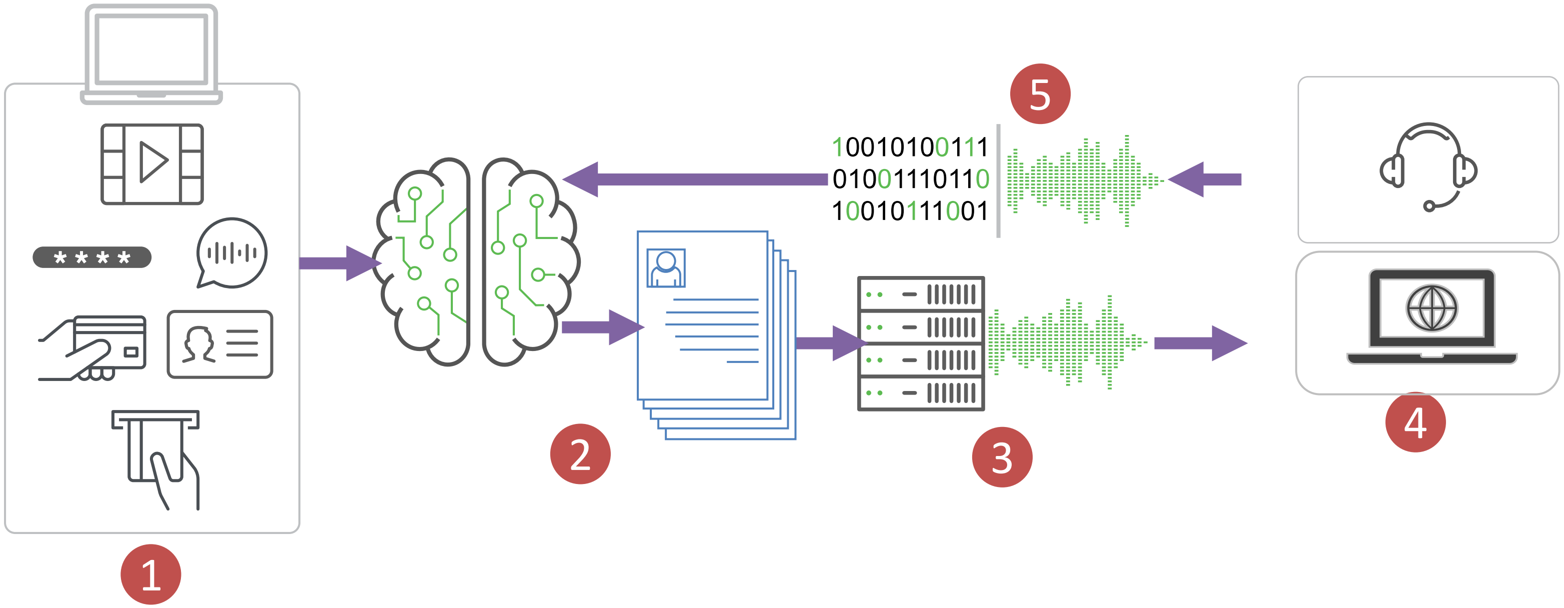
WHICH IS FAKE?

WHICH IS FAKE?

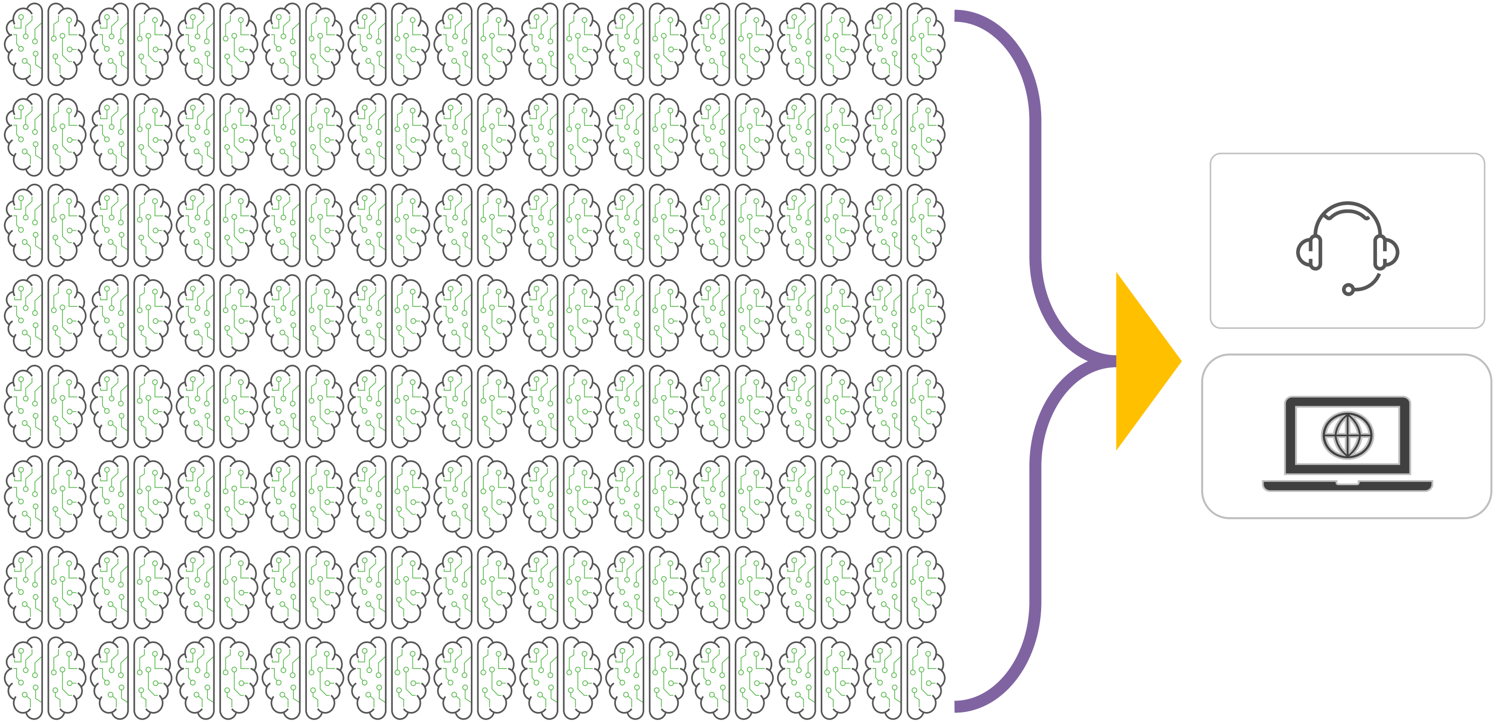
HUMANS HAVE BEEN THE BOTTLENECK TO FRAUD TO DATE



NEW TECHNOLOGIES ARE ENABLING NEW TYPES OF ATTACK…



AI Powered Fraud can Scale… Faster



Mitigating Artificial Intelligence Risks

- Monitor your system effectiveness for capturing fraud. AI learns the gaps, but monitoring the system allows you opportunity to close gaps quickly and aggressively.
- Establish strong manual process quality assurance testing. Human error is the key to allowing fraud. AI will find the controls that are not being followed.
- Change and/or adjust your thresholds for fraud review. The AI system will find the point where a transaction is reviewed and target below this threshold.
- Establish vendor meetings to understand the vendor’s ability to capture AI fraud attacks.

QUESTIONS

Patrick Smith
psmith@aba.com

Additional Resources

- CISA has several resources:

  https://cisa.gov/cybersecurity

  https://cisa.gov/stopransomware

- USSS Preparing for a Cyber Incident includes several resources:
  https://www.secretservice.gov/investigation/Preparing-for-a-Cyber-Incident

- FBI IC3:

  https://www.ic3.gov/

- Federal Reserve Bank Synthetic ID Toolkit

  https://fedpaymentsimprovement.org/synthetic-identity-fraud-mitigation-toolkit/synthetic-identity-fraud-basics/