Building Success. Together.

Agenda

I. Fraud Risks
II. Fraud as a service
III. Social Engineering
IV. Check Fraud
V. AI
VI. Questions

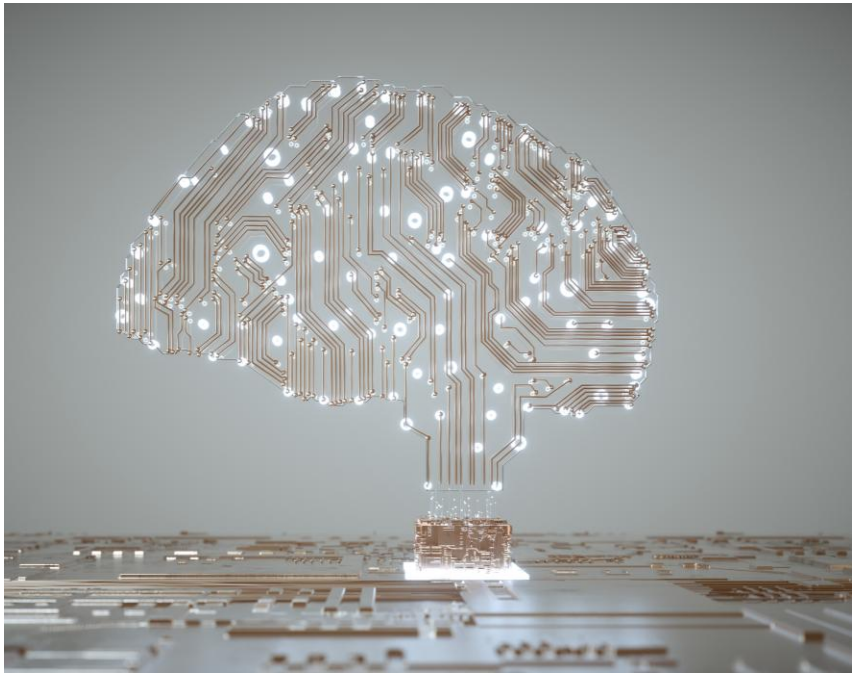
FRAUD RISK IMPACTS

Over $1 trillion USD in financial losses globally due to scams.

60% of financial institutions reported an increase in fraud risks from 2023 to 2024, with the largest growth in enterprise banks

Over 50% of fraud cases now involve AI technologies.

FRAUD RISK IMPACTS



- **Generative AI scams exploded**: Global scam losses reached **$1 trillion in 2024**. Breached personal data surged **186% in Q1 2025**, with phishing reports jumping **466%**. Between May 2024 and April 2025, GenAI-enabled scams rose **456%**, and **82% of phishing emails** are now AI-generated.

- **Widespread use of AI in fraud**: Over **50% of fraud involves AI**. Among fraud professionals: **92% report criminals use GenAI**; **56% cite AI-powered social engineering**, **44% note deepfakes.**

FRAUD AS A SERVICE (FaaS)

Criminals outsource fraud capabilities through encrypted online marketplaces.

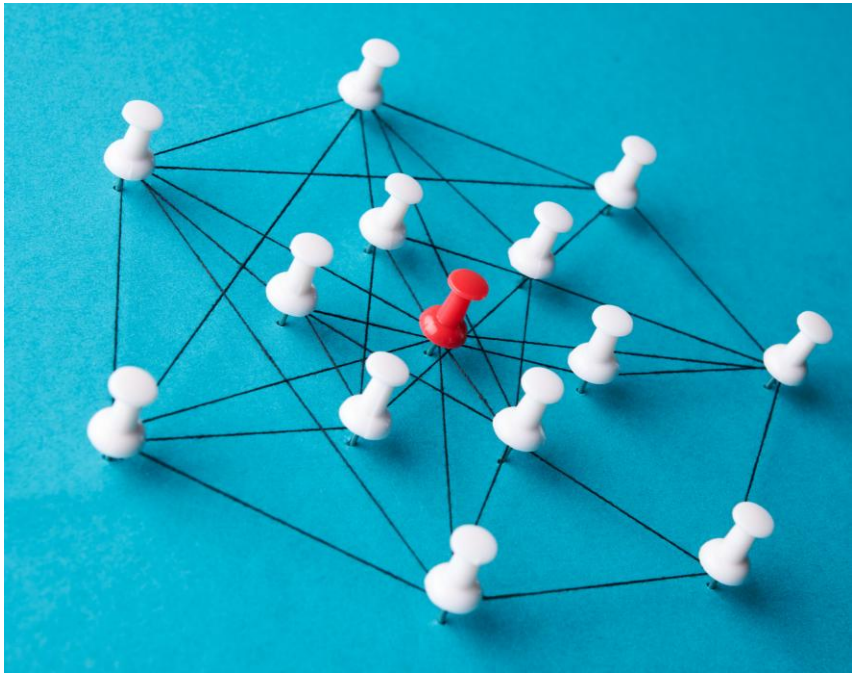
Criminals develop, package and sell fraudulent tools or services, allowing others to execute scams or financial crimes.

This lowers the skill barrier to financial crime and cybercrime.

Ways FaaS Commit Fraud

- **Phishing Kits** – prebuilt templates that mimic senders
- **Malware** – subscription-based access to malicious software
- **Credential stuffing tools** – automated programs for testing stolen usernames and passwords
- **Botnets for hire** – networks of compromised computers
- **Synthetic identity generators** – tools that combine real and fake personal information for new identities
- **Money mule networks** – services to launder funds
- **Call centers "spoofing" services** – voice-based operations that impersonate legitimate institutions

SOCIAL ENGINEERING



Trust accounts are often set up in a structure involving multiple parties (trustee, beneficiaries, attorneys and fiduciaries), operating under specific document and ad hoc instructions.

This complexity creates multiple human touchpoints that can be compromised through social engineering scams.

Basics of Social Engineering

Select the Victim

Build Trust

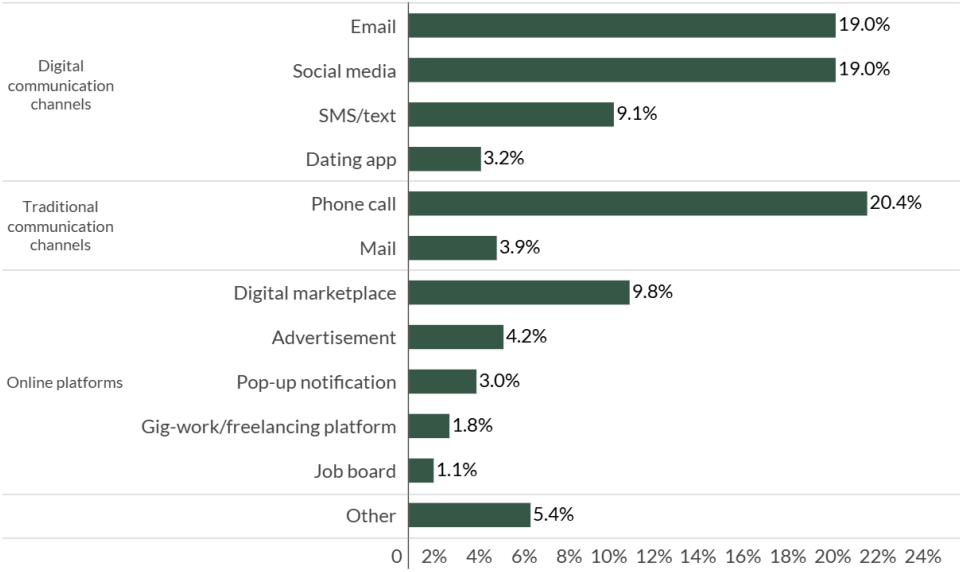
Create Fear

Make the Pitch

Scams Landscape

Scammers' channels for initial contact

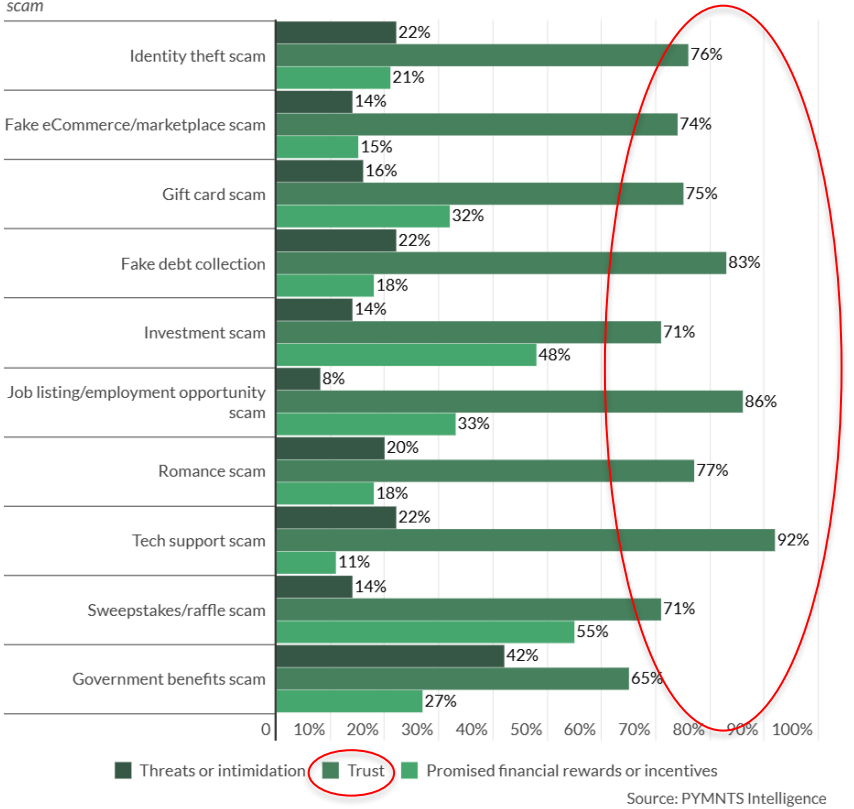
Share of financial scam victims reporting scammers made first contact through select channels



Source: PYMNTS Intelligence
How Scammers Tailor Financial Scams to Individual Consumer Vulnerabilities, January 2025
N = 2,209: Respondents who have experienced household financial loss because of a scam, fielded July 26, 2024 – Aug. 19, 2024

Financial scam compliance tactics

Share of financial scam victims reporting select tactics that scammers used to gain their compliance, by type of scam



Source: PYMNTS Intelligence
How Scammers Tailor Financial Scams to Individual Consumer Vulnerabilities, January 2025

SOCIAL ENGINEERING RED FLAGS

- Engage
  - Mimic a trusted environment
  - Imply rewards
  - Express common interests
  - Make the target feel important, but not exposed or responsible
  - Create a sense of partnership
  - **Create a sense of urgency**

- Avoid
  - Imply or express consequences
  - Aggressive and confrontational tone/language
  - Isolate the target from any outside influence
  - Remove options/alternate solutions
  - **Create a sense of urgency**

MITIGATION

Client Education – Increase the awareness of social engineering for all parties to the trust

Multi-layer verification and authorization – Develop dual authorization processes, unique verification methods and manual “call-back” step-up procedures

Monitor accounts – Look for anomalies in the account and report them to the bank immediately.

Pause – Social engineering requires the person to react from instinct or emotion. Pausing allows the objective analysis of the situation.

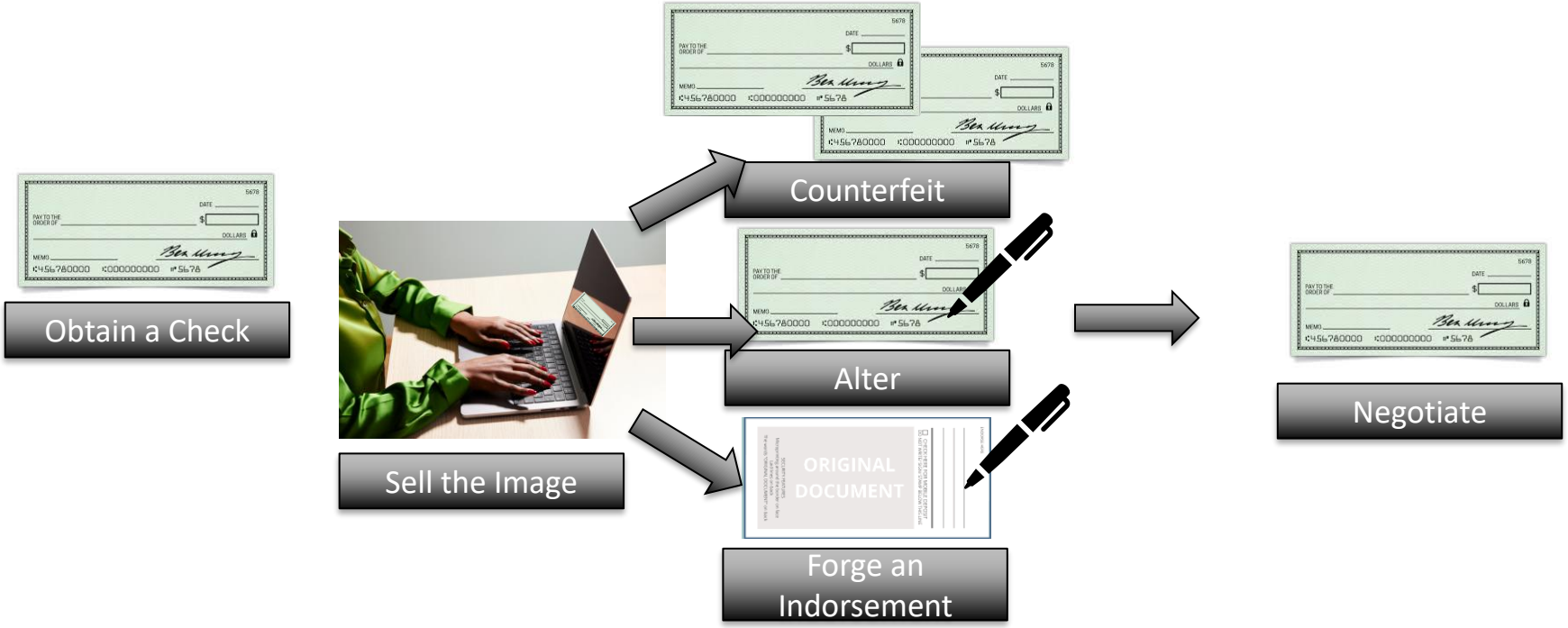
CHECK FRAUD

Many trust arrangements have long relied on paper checks as the default disbursement method.

Checks are established as a record of payment, accounting practice and familiar document.

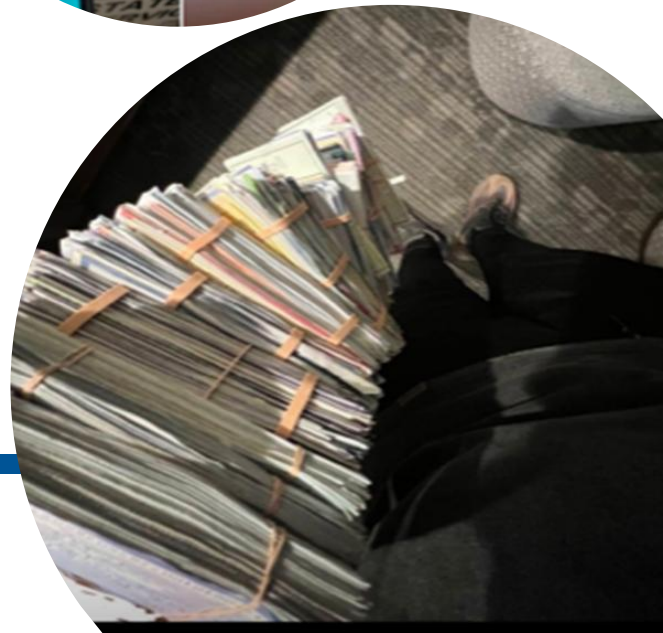
Checks represent the **least secure** method of payment currently available for disbursements.

BASICS OF CHECK FRAUD



Check Fraud

- Check fraud accounted for **66% of payment fraud**, followed by 37% for ACH debit fraud.
- FinCEN Sep 2024 Check Fraud Analysis – Claim Type
  - 44 percent were altered and then deposited
  - 26 percent were used as templates to create counterfeit checks
  - 20 percent were fraudulently signed and deposited
- **$688 Million in Check Fraud SARs over Six Months**
- The primary source of check fraud is the **United States Postal System,** compromised by fraud gangs and their theft of **Arrow Keys**.

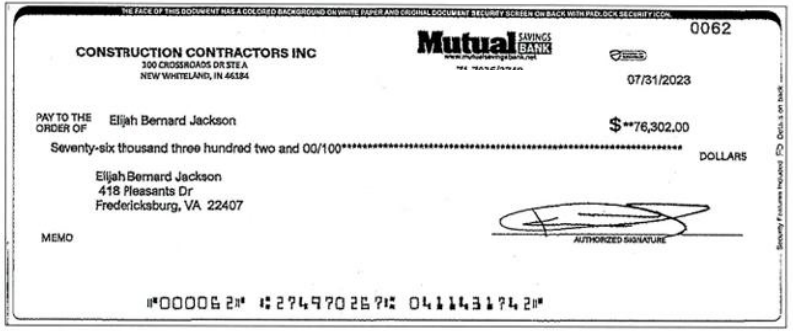


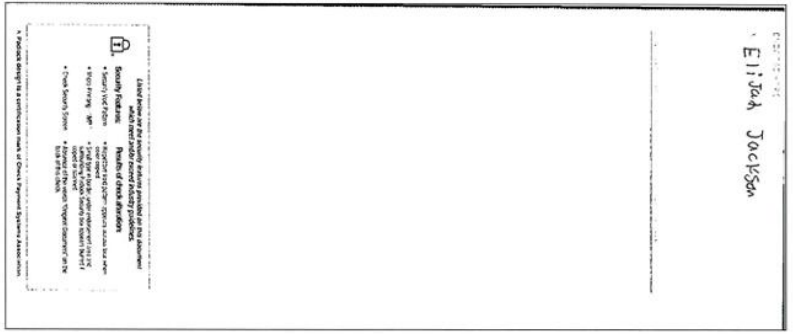
WHY IS CHECK FRAUD DIFFICULT TO MANAGE?

- Advances in imaging software and check washing techniques make identifying differences in altered and counterfeit checks difficult.
- The ability to create a business account to use as a mule accounts for checks is easier with the availability of information on the internet.
- Banks are focused on the management of liability between the Bank of Deposit and the Payee bank.

Mitigation: Protecting Customers and Banks

- Customer messaging
  - Minimize use of checks
  - Move toward electronic payments/payroll
  - Do not use blue mailboxes
  - Watch accounts closely
- Banks
  - Require use of positive pay or have customer sign indemnification agreement
  - Ask core to review check fraud capabilities
  - Relook funds availability for all channels
  - Review all check transactions the day they arrive
  - Ensure staff is trained on all tools (collections)
  - RDC checks not subject to Reg CC hold times!





https://www.aba.com/-/media/documents/reference-and-guides/from-the-compliance-hotline.pdf
Page 89

FRAUD ENHANCED BY AI

- AI is a tool. It makes the traditional fraud risks rapid, efficient and agile.
  - Phishing/Spoofing
  - Account Compromise
  - Verification/Authentication Compromise
  - False Documents
  - Deepfake

AI Driven Tools Enable Better Scams

Generate background sounds using text prompt “Thunderstorm with heavy rain”

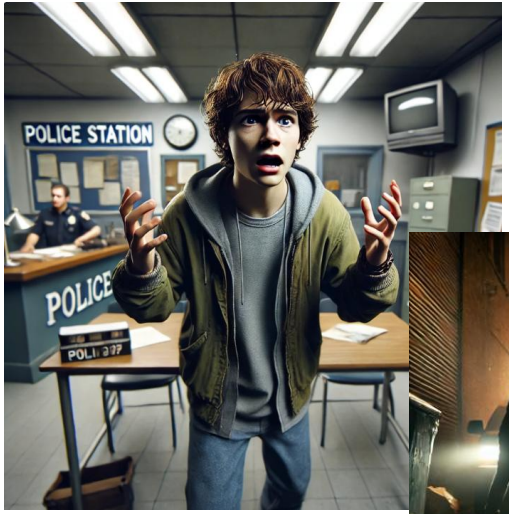
Step 1: Obtain copy of child’s voice

Step 2: Use tools to clone the voice

Step 3: Create convincing script that the child is in need of help/money.

Step 4: Execute script with cloned voice

Step 5: Merge cloned voice with realistic background sound



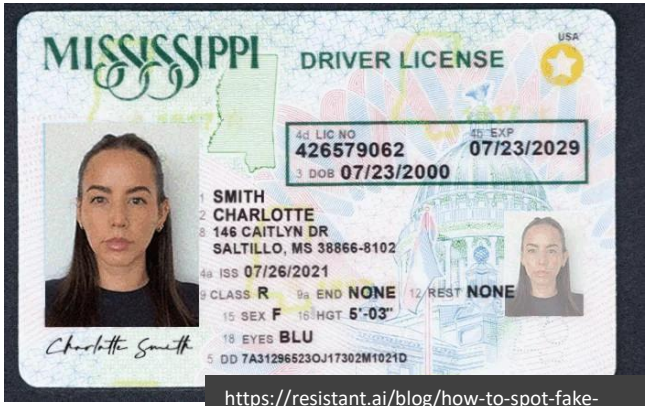
https://www.wsj.com/tech/personal-tech/the-panicked-voice-on-the-phone-sounded-like-her-daughter-it-wasnt-8d04cbc1?st=wBLoHh&reflink=desktopwebshare_permalink

FALSE DOCUMENTATION

Only Fake is a website dedicated to making convincing ID documents.

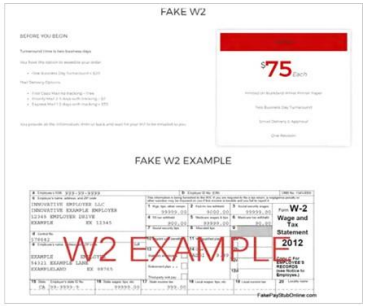
This includes:

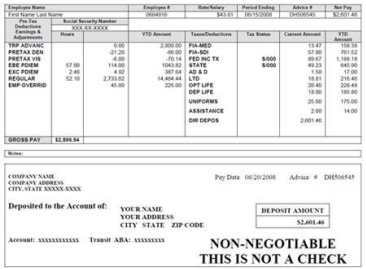
- Text
- Portrait
- Signature
- Hologram
- Machine Readable Metrics
- ID Template
- Background

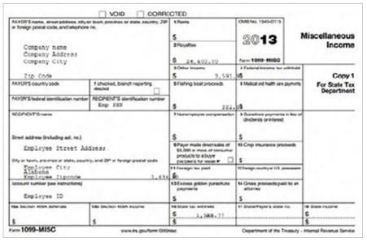


https://resistant.ai/blog/how-to-spot-fake-documents

https://regulaforensics.com/blog/forged-documents/







AI FRAUD MITIGATION

- Increase your staff/client awareness using recent fraud events.
  - The Red Flags for a fraud event can be sophisticated and require real examples to ensure effective understanding.
- Layer your defenses.
  - Stacking system defenses and manual processes makes fraud against your institution more expensive.
- Know your customer.
  - Beyond just validating the identity, a true conversation with a customer arms you with information that AI will find difficult to replicate.
- Meet with your Vendors.
  - AI is a tool to catch fraud as much as it is to enhance fraud. Understand how your vendors are currently situated in the market.

QUESTIONS?

Additional Resources

- ABA is leading the industry in educating bank staff and the public on scams and arming banks with resources. Below are some of our offerings.
- **ABA Fraud Directory** - helps banks connect with other institutions to resolve warranty breach claims for checks as well as claims for unauthorized and/or fraudulent transfers for wires, ACH, RTP, or FedNow.
- ABA **Fraudcast** – cyber and fraud podcast with Paul Benda.
- **Banks Never Ask That** – our award-winning anti-phishing campaign which includes videos and graphics that banks can put on their websites and social media to equip the public
- **Practice Safe Checks** – our newest (check fraud) campaign
- **Treasury Check Verification System** – The system will support the verification of most federal government-issued checks, including, but not limited to social security payments, federal salary checks and economic stimulus payments.
- **Infographics on Crypto Scams** – for bank staff and their customers; developed in partnership with the FBI, Department of Homeland Security, Secret Service, etc.
- **Infographic on Check Washing and Check Theft Scams**
- **ABA Ransomware Toolkit** - easy-to-follow guides on how to protect your system, understand the pros and cons of paying a ransom, and how to respond quickly.
- **ABA's 4-Person Cyber & Fraud Team of Experts** – led by Paul Benda, EVP of Risk, Fraud, & Cyber, Paul and his team offer free 1-on-1 guidance to members as well as formal presentations on request
- **Fraud Committees & Working Groups** – see ABA's Committee Directory
- **Numerous Webinars including** Mitigating Loss: Understanding the Fraud Triangle, Why Banks are Banking on Identity, Unmasking Deepfakes: Preventing AI-Driven Deepfake Fraud at Your Bank, and Hot Topics in Sanctions Requirements and Enforcement Actions.
- **Content-Rich Fraud Pages –** such as Fraud, Tax Refund Fraud, Identity Theft, Elder Financial Exploitation
- **Safe Banking for Seniors –** financial education program for banks to deliver locally
- **Advocacy & Congressional Testimony**
- **Articles, Data, & News**

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/

Articles:
- Datavisor: Top Fraud Trends and Predictions for 2025 – And How Will the Industry Respond? February 14, 2025.
- Alloy: Alloy's 2025 State of Fraud Report