American Bankers Association

Building Success. Together.

# Preventing Fraud: Moving More to Prevention than Reaction

This presentation will cover:

1. Fraud Statistics
2. Fraud Operations
3. What is in your control vs what is outside of your control
4. How is prevention accomplished
5. Questions

# KEY STATISTICS

1. **Check fraud** remains the largest fraud-loss category, accounting for 43.3% of fraud value despite a declining check ecosystem.

2. **Domestic wire fraud** increased to 34.3% of total fraud value, reflecting a migration toward higher-value account-to-account fraud.

3. **ACH fraud** is the fastest-growing payment fraud threat, with fraud value increasing 52% year-over-year while transaction value increased only 11%.

4. **P2P (Zelle)** continues to generate the majority of fraud attempts, representing 65% of fraud volume, but only 0.8% of fraud value.

5. More than 50% of fraud now originates from **trusted devices**, eroding a traditional fraud-detection pillar.

# CHANNEL PRESERENCES

Web fraud rate increased 22% (15.6% → 19%) Consumers are roughly 3x more likely to experience **account takeover** on web channels.

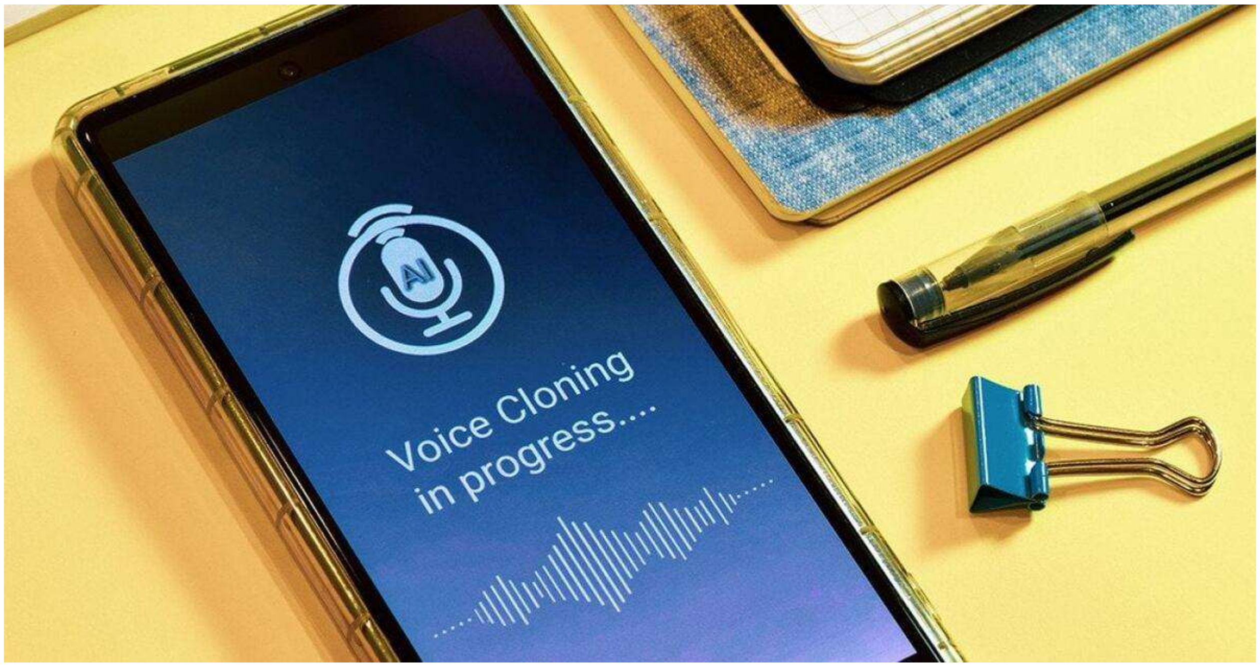
Mobile users are approximately two-thirds more likely to experience **authorized scam** fraud

# AI ENABLED FRAUD

## AI-Enabled Fraud Emerged as a Major Threat

- For the first time, IC3 separately tracked AI-enabled fraud.
  - 22,364 complaints
  - $893 million in reported losses
  - Estimated true losses of $6.3 billion using the report's methodology.
- This is one of the strongest indicators that generative AI is beginning to materially impact fraud victimization.

# KNOWN TO ME STANDARDS ARE NO LONGER EFFECTIVE




Voice over

Risk

Attempt

Original

# FRAUD OPERATIONS – Built to Respond

Fraud Operations groups are largely evaluated on loss and fraud attempt metrics.

↓

Fraud metrics are built on events that have occurred and have been tagged “fraud”.

↓

Controls are built on identified control gaps and inefficiencies.

↓

Oftentimes new controls may remove older controls

# GAPS IN A REACTIVE MODEL

- Fraud attempts are agile, quick and can evolve in seconds.
- Fraud reaction depends on the identification of an attack vector
- The identification can delay controls beyond a new control effectiveness
- Attacks can learn to circumvent controls outside of a direct attack on your bank

# WHAT IS IN YOUR CONTROL

**VETTING YOUR CUSTOMER**

**ACCESSING YOUR ONLINE AND MOBILE BANKING**

**STANDARDS FOR A VALID TRANSACTION (AUTHENTICATION AND VERIFICATION)**

**HOLD PERIODS (SUBJECT TO REGULATIONS)**

**ESTABLISHING "REASONABLE SECURITY" OPTIONS**

# WHAT IS NOT IN YOUR CONTROL

- Criminals directly reaching out to your client
- Business Email and Vendor Invoice compromises
- Spoofed bank phone and text messages
- Fake vendor ads

# MOVING TO PREVENTION

**Learn from attempts on the industry, not just attempts on your bank**

**Have Fraud Operations as a stakeholder in any new products or changes to the client experience**

Fraud Operations is the voice of potential control gaps to criminal activity

**Assess processes to ensure the preservation of effective controls**

**Educate clients on recent trends in scams and frauds**

**Educate your staff on fraud risks**

**Set client communication standards to recognize specific needs for a socially engineered client**

# HOW CAN THE INDUSTRY PARTNER TO HELP

- Trades and Associations are actively influencing regulation and legislation to enable stronger consumer and bank fraud risk management
- Telecommunication bills are presented to hold telecom companies to standards of preventing spoofed calls and taking down SIM farms
- Online advertising platforms are facing pressure from legislation and industry voices to establish fraud advertisement controls
- Information sharing forums are expanding their membership and focus to allow for greater bank to bank exchange of practices

# 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