



Building Success. Together.

1

Agenda Items

1. Fraud and Scam Trends
 - Ransomware
 - P2P / Bank Impersonation
 - ABA Scam Mitigation Efforts
2. Check Fraud
 - Trends
 - Mitigation Measures
3. AI in Fraud and Mitigation Strategies

2

Top Cyber Attack Tactics



Third-party attacks (e.g., Solarwinds in 2019)



Zero-day vulnerability exploits due to the increasing attack surface caused by digitization of the financial sector



Ransomware attacks (e.g., Nov 2023 U.S. division of ICBC led to significant disruption in Treasury markets)



Social engineering such as phishing (including QR code phishing) and business email compromise (BEC)



Distributed denial of service (DDoS) attacks



Breaches

3

2024 Verizon Breach Report



- All Industries
 - 68% of all breaches involve human element (down 6% from 2023)
 - 65% are external actors (but internal actors are rising)
 - 28% of breaches involved errors and 15% of breaches involved a 3rd party
 - Most popular methods used by external actors: stolen credentials, phishing, exploit vulnerabilities
 - About 1/3 of all breaches involved ransomware or some other extortion technique.
 - Over 90% of attacks observed last year were financially motivated
 - Espionage as a motive increased from 5% to 7%

Report: <https://www.verizon.com/business/resources/reports/dbir/2024/summary-of-findings/>. Verizon has been producing these reports since 2010.

4

IBM "Cost of a Data Breach Report 2024"



- \$4.9 million average (10% increase from previous year)
- Average breach took **169 days to identify** and another **58 days to contain**
- **Healthcare sector** saw the highest costs from breaches, **averaging \$9.8 million per incident, followed by financial services at \$6.1 million**
- 17 of the breached organizations surveyed suffered what IBM classified as a "mega breach" **involving 1 million+ records**
- Of the breached organizations surveyed, **63% said they plan to increase their security spending, up from 51% the previous year**
- Organizations that worked with law enforcement spent **on avg. \$1 million less**, not including any ransom paid

Source: [Cost of a data breach 2024 | IBM](#) and based on research conducted by Ponemon Institute and survey of 604 organizations across 17 different industries and 16 countries or regions that suffered data breaches between March 2023 and February 2024

FBI IC3 – 2023 Internet Crime Report

Complaints and Losses over the Last Five Years*



- 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 2021³⁶

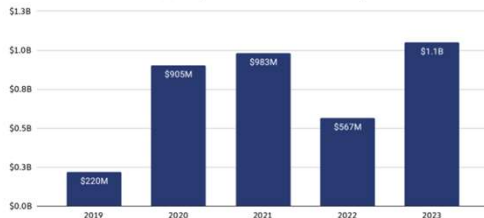
Typology	Number of BSA reports	Total Suspicious Amounts
General Fraud	1.2 million	\$149 billion
False Records	-423,000	\$45 billion
Identity Theft	-222,000	\$36 billion
Third-Party Money Laundering	-154,000	\$18 billion
Circumventing Standards	-110,000	\$12 billion
Total	2.1 million	\$260 billion

- Some of the best estimates of total fraud can come from SARs
- TOTAL Identity Related SARS Filed - **\$351 Billion**
- FTC estimates 2023 could be as high as **\$158 Billion**

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

7

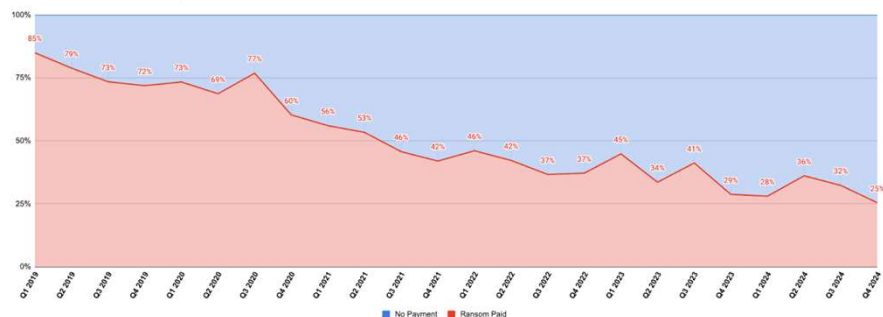
Total value received by ransomware attackers, 2019 - 2023



Ransomware – Good and Bad News

- 2023 a record year
- Firms getting better at protecting themselves – Q1 2019 85% paid Q4 2024 25% paid

All Ransomware Payment Resolution Rates



8

Law Enforcement Can Make a Difference

Top RaaS strains by ransomware revenue, 2022 - 2023



- Ransomware payment volumes
- FBI infiltrated notorious ransomware gang
- Significantly impacted flow of payments
- Estimate reduced ransomware payments by \$210.4M

9

Scams Landscape

Scammers' channels for initial contact

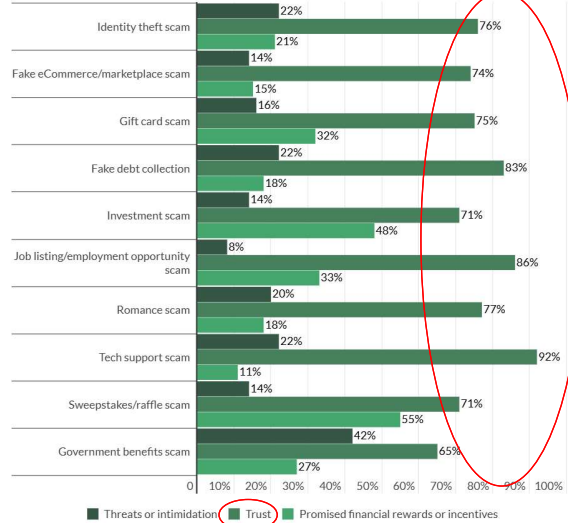
Share of financial scam victims reporting scammers made first contact through select channels



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

10

Blocked
Unblock to receive messages from this sender

Unblock



Dr. Jack, this is my photo. I hope you can reply to me as soon as possible after seeing my message, because I have a tooth problem and am very uncomfortable. I need your help as soon as possible. If you have time, I hope we can confirm an appointment

Text message

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

aba.com | 1-800-BANKERS

11




11

ABA Fraud Mitigation Efforts

Operational	Ongoing	Proposed
ABA Fraud Contact Directory	ABA Fraud Indicator eXchange (FIX)	Updated Check Security Measures
Check Fraud Efforts (toolkit, training, ed partnerships, working groups)	ABA Freeze Framework	Payee Confirmation Program (electronic transfers)
Bank Programs to Stop Spoofing – FCC Engagement	Legislative Asks (to require other industries and the government to assist in combatting scams and fraud)	Updated Frontline Training for Scam Interventions
#BanksNeverAskThat and #PracticeSafeChecks Campaigns	Engagement with Treasury on Treasury Check Fraud	Strengthening KYC for New and Updated Business Registrations
ABA Foundation work: Safe Banking For Seniors Program	National Check Verification System Feasibility Study	

aba.com | 1-800-BANKERS

12



12

Mitigation Efforts – Updated Messaging

- Scams and fraud are a huge problem
- Banks do more than any industry to protect their customers but can't do it by themselves
- Tell people don't send money to people you don't know and trust but by the time they're making that payment they believe they know and trust who talking too
- Need to focus on scam prevention
- Shared responsibility
- Telecoms and social media companies are enabling the scammers and profiting from the scam ecosystem

13

Mitigation Efforts – Our Asks

- Establish a White House Office of Fraud and Scam Prevention
 - Develop a National Strategy to prevent fraud
 - Don't want it in Treasury because makes it appear that it's a bank problem to solve
 - Modeled after Office National Cyber Director – no regulatory authority
- FCC increase enforcement and establish database of customer reported spam texts
 - Lobbying on current rule focused on email to text and blocking at originating
 - Sending a letter asking for establishment of spam text database
 - Focus on enforcement of spoofed caller IDs
 - Develop SLA for takedown requests of bad numbers and social media profiles
- Bring state and local law enforcement to the fight and improve prosecution rates
 - Replicate TX FCIC model
 - Work with the National White Collar Crime Center to develop templates to prosecute cases

14

Operational Mitigation - Fraud Contact Directory

- Nearly half of all banks participating in the Directory
- Adding credit unions to the Directory – planned April
 - Budget approved and developing technical solution
 - Finalizing validation procedures
 - Validation procedures will determine extent of participation
- Developing “Freeze Framework”
 - Standardized procedures around requests to freeze/hold funds from fraudulent transfer
 - Establishment of Universal Indemnity document
 - Several legal and compliance issues must be addressed

15

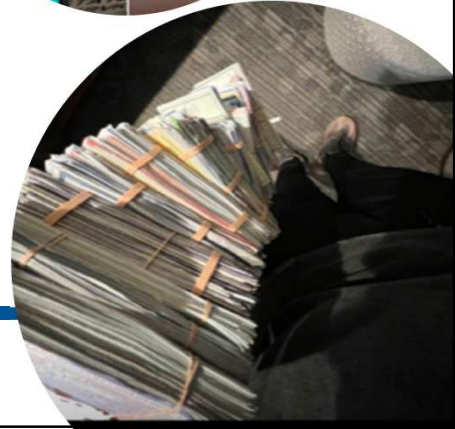
Ongoing Fraud Mitigation Efforts

- ABA Fraud Indicator Exchange
 - Prevent the flow of funds to criminals
 - Performing proof of concept historical analysis
 - Deployment planned for first part of next year
- #BanksNeverAskThat campaign and #PracticeSafeChecks
 - Nearly 2000 banks participating
 - Media efforts reached nearly 4 Million in TV and 12 Million for radio
 - Additional resources for holiday season
- Enhance international partnerships

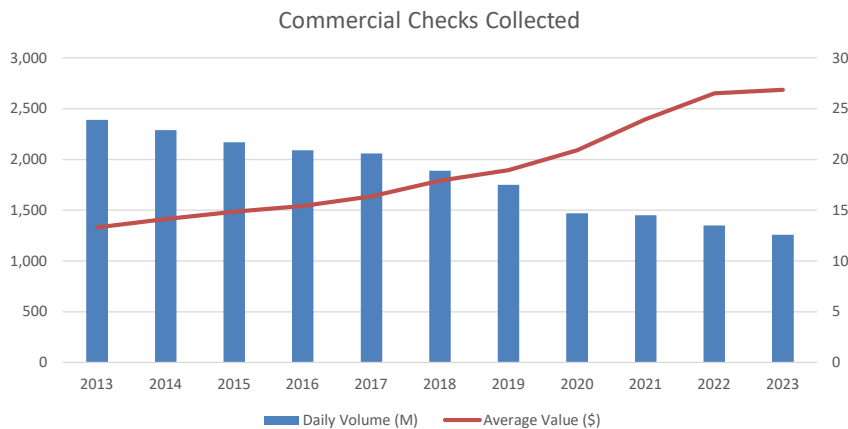
16

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**.

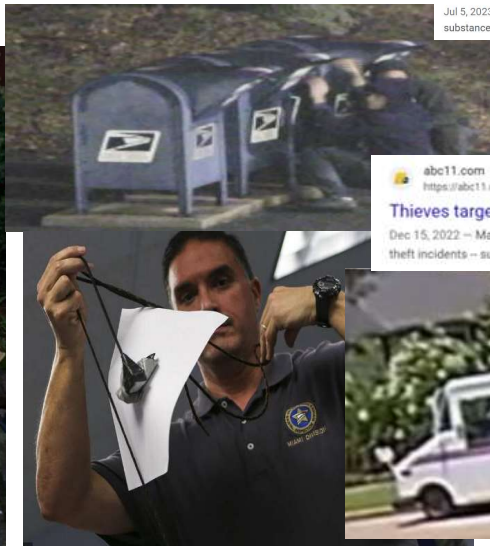


People Still use Checks – but less



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

Mail Theft Evolution



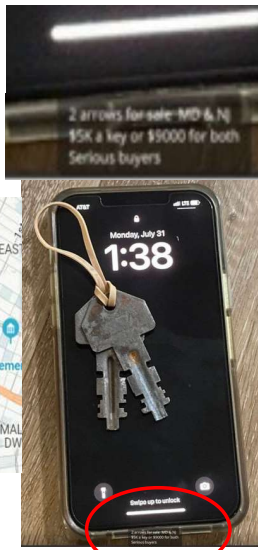
USA Today
https://www.usatoday.com › money › 2023/07/05 › us...
U.S. Postal Service theft, mail carrier robberies on rise. ...
Jul 5, 2023 — Should you be concerned about mail theft? · Glue traps. Thieves use a sticky substance on the door of the mail box to catch mail, which they can ...

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 — Mairon said thieves are getting the stolen checks by either swiping ... in mail theft incidents -- such as mailbox thefts and postal carrier ...



This arrow key was for purchase at price of \$4,000 on telegram. It's designed to unlock USPS boxes within 10013 zip code



Mail Theft At-A-Glance

- Agency priority for USPIS, in partnership with USPS
- Motivated by financial gain
- Investigations are resource intensive and present many challenges
 - Minimum Exposure and Loss Thresholds for Federal Prosecution
 - Cyber-enabled with national reach
- There are **139,868** blue collection boxes
- USPIS relies heavily on law enforcement agency partnerships and cooperation from financial institutions



Order Counterfeits or Make Your Own!

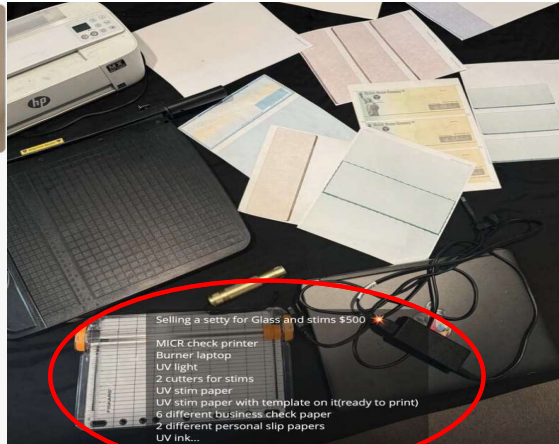


(UV HOLOGRAM, WATERMARK, & MICR INCLUDED)
 \$500
 PICK UP OR NEXT DAY SHIPPING

When Placing Order Please Make Sure To Provide

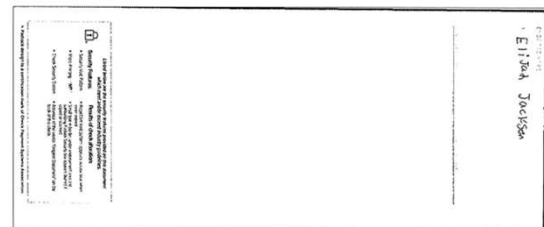
- FULL CORRECT NAME
- FULL CORRECT ADDRESS
- CLEAR PHOTO OF ORIGINAL STIM

ONCE CONFIRMED & PRINTED THERE'S NO REDO'S FOR FREE !!



Messaging: 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!

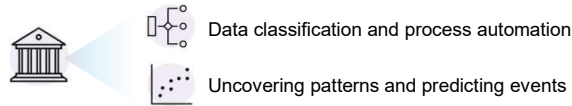


<https://www.aba.com/-/media/documents/reference-and-guides/from-the-compliance-hotline.pdf>
Page 89

Check Fraud Mitigation Efforts - Industry

- Payee confirmation for Treasury checks
 - Only through API now – banks onboarding now
 - ABA exploring ability to host API interface for banks
- Performing National Check Verification System Feasibility Study
 - Basically TCVS for commercial and consumer checks
 - Build vendor agnostic framework
 - First meeting in March and final report released at ABA Financial Crimes Conference
- ABA Resources
 - ABA Fraud Contact Directory
 - ABA Check Fraud Toolkit and Frontline Course
 - ABA Check Fraud Product Assessment

Banks have been using traditional AI for years



<p>Credit scoring: statistical models for assessing creditworthiness</p>	<p>Fraud detection: analyze transaction patterns</p>	<p>Customer segmentation: based on behavior for targeted marketing</p>
<p>Risk assessment: predicting loan default risk</p>	<p>Process automation: data entry or account reconciliation</p>	

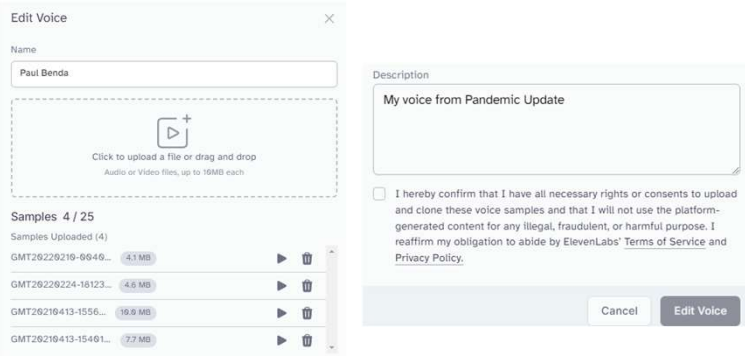
There are risks to *banks* using GenAI

While AI has the potential to revolutionize banking, its misuse can lead to serious problems.

Data privacy		11% of data employees paste into ChatGPT is confidential
Misinterpretation of complex queries leading to incorrect advice		Example: "An AI assistant recommended high-risk investments to conservative clients due to misinterpreting risk tolerance questions."
Generation of biased content		Example: "An AI-generated marketing campaign unintentionally used language that excluded certain demographic groups."
Overestimation of AI capabilities leading to underdeveloped products		Example: "A new AI-driven loan approval system failed to account for important human factors, leading to unfair rejections."
Accuracy and hallucination		Example: "The branch is open 24 hours, days per week."

Accessible Voice Deepfakes

- For \$1 you can buy a month-long subscription to Eleven labs and clone any voice you have recorded



This is a copy of my voice



Which voice is real?

Where it gets scary
ABA CEO Rob Nichols copied



Created with publicly accessible YouTube clips

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



Advances in AI Deep Fake Technologies



Video Source of Screen Grab

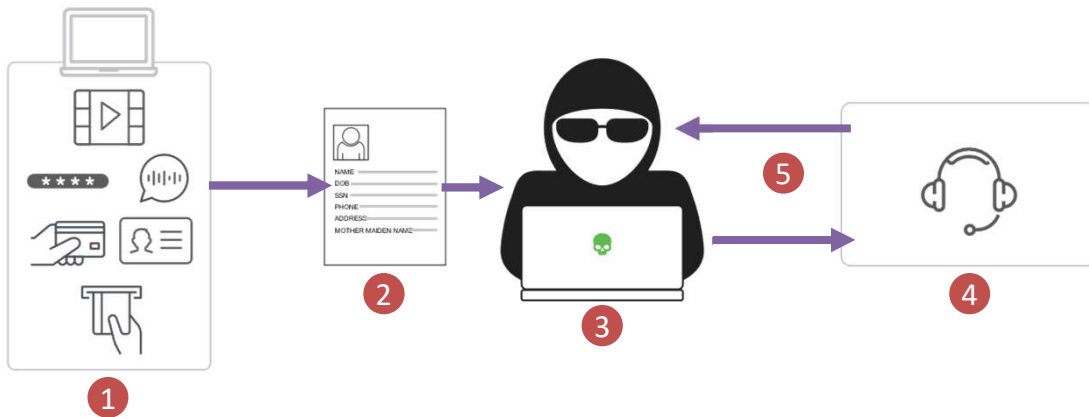


Use the image and copy the voice - turns into something nefarious

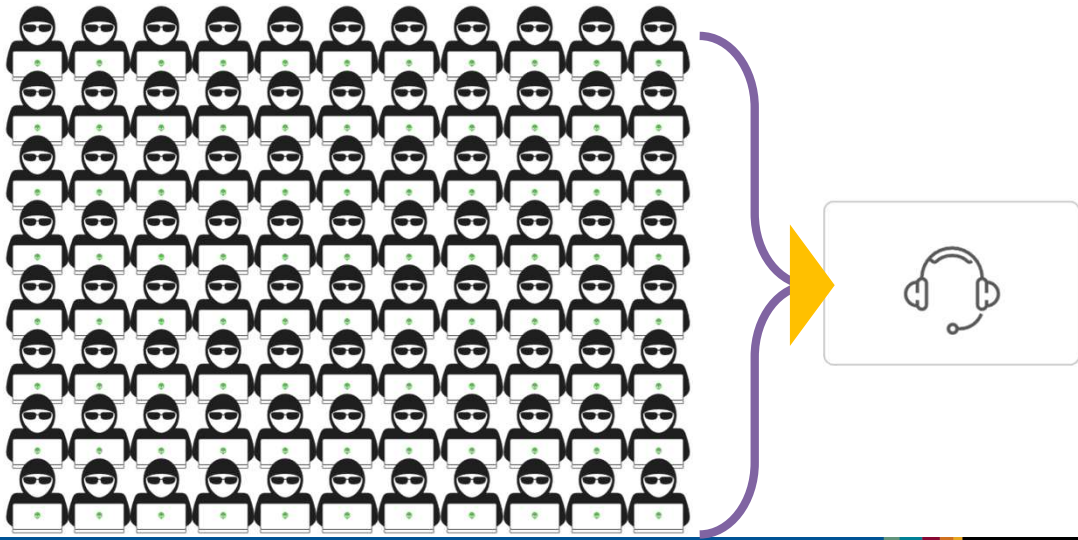
Or, something funny



CLASSIC FRAUD IS ANNOYING...

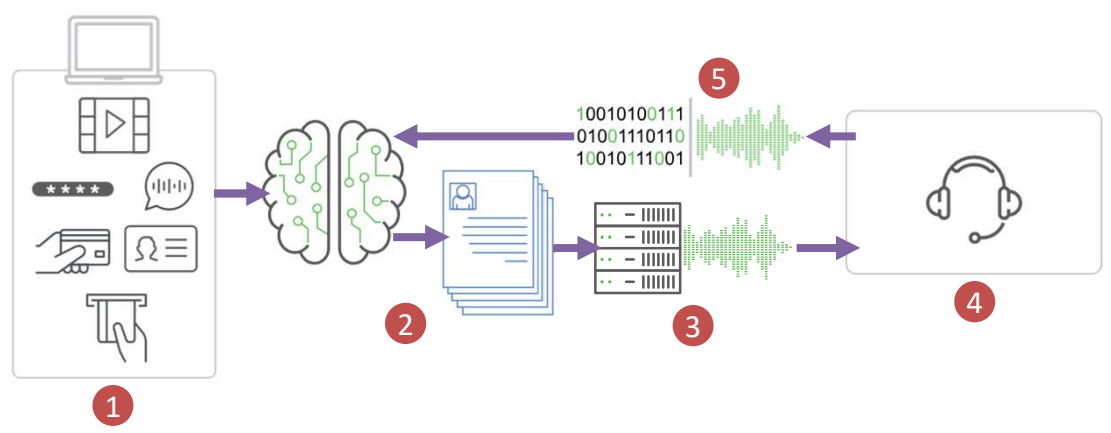


HUMANS HAVE BEEN THE BOTTLENECK TO FRAUD TO DATE



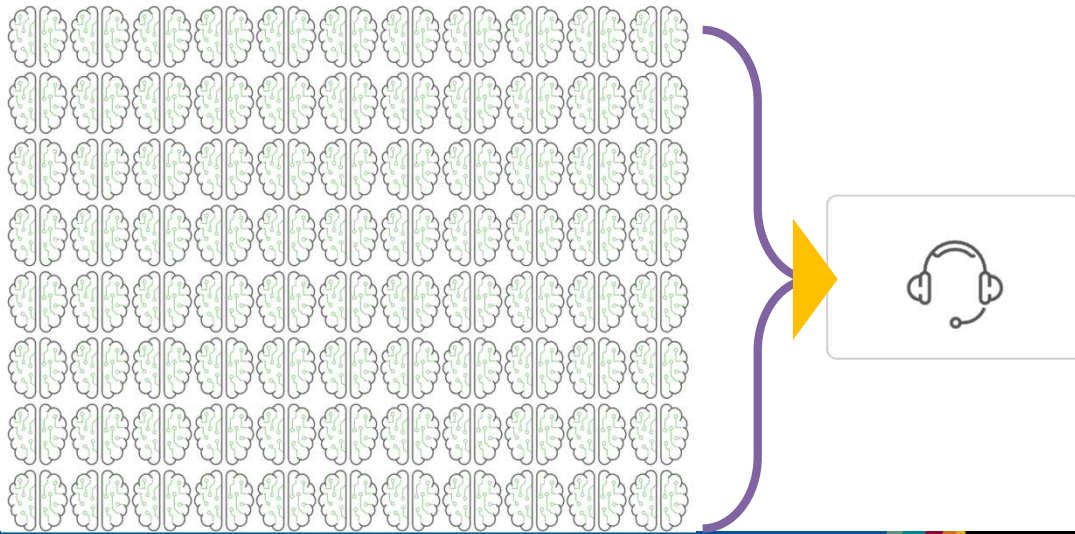
31

NEW TECHNOLOGIES ARE ENABLING NEW TYPES OF ATTACK...

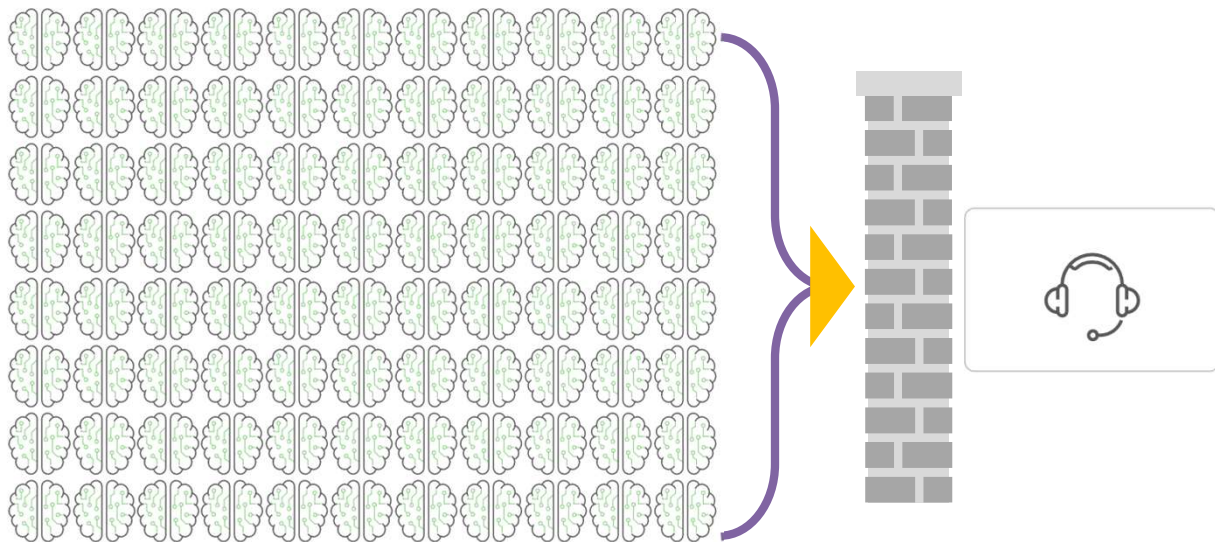


32

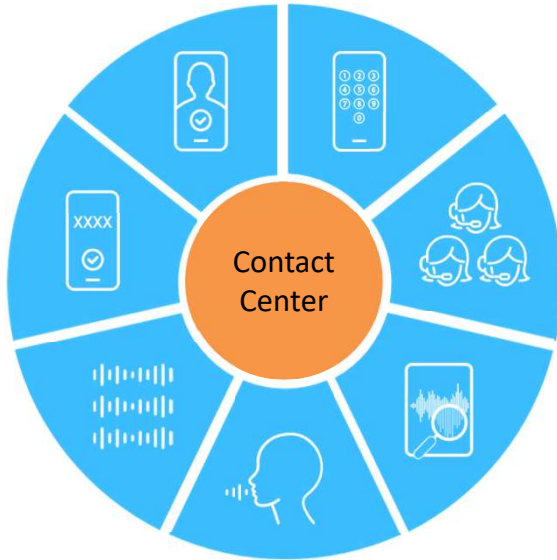
AI POWERED DEEPFAKES CAN SCALE AND FASTER





AI POWERED DEEPFAKES CAN SCALE AND FASTER





LAYERED DEFENSE AGAINST DEEPFAKES





-  Phone/Device Signals


-  Contact Center
Staff Best Practices Education

-  Adaptive Synthetic Voice Detection
(Deepfake Firewall/Antivirus)

-  Speaker Voice Authentication

-  Voice Replay Detection

-  Device/App Based Authentication

-  App-based Biometric Authentication

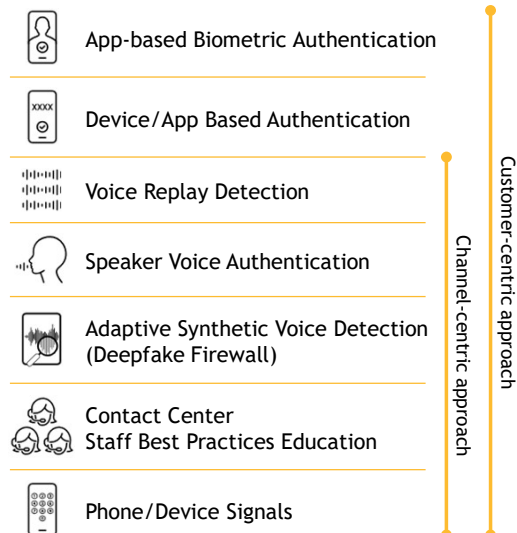
AN AI-POWERED COMPREHENSIVE DEFENSE

Organizations need a comprehensive approach to defending against deepfakes (at scale)

Continuous research, analysis and adaptation to ensure rapid response to emerging threats

Each technique can be deployed independently or combined in a multi-technique “fusion” approach.

- Scores from techniques evaluated as part of overall risk framework



Additional Resources

- ABA Banker Working Groups
 - National Best Practices Fraud Group
 - Reg E / Card Information Sharing Group
 - Check Fraud Working Group
 - Internal Fraud Group
- ABA Fraudcast - aba.com/fraudcast
- 1-800-BANKERS

QUESTIONS

Paul Benda
pbenda@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/>