MARYLAND BANKERS ASSOCIATION

Bank Operations and Cybersecurity

Mr. John Carlson, Mr. Stephen Kenneally, and Mr. Patrick Smith
American Bankers Association

Cybersecurity and AI Update
Maryland Bankers Association
August 8, 2024

John Carlson
American Bankers Association

Agenda

- Cyber Risks
- Regulatory issues
  - Incident notification
  - Third Party Risk Management
    - Cloud computing
- Unique Public-Private Collaboration, Standards and Executive Orders:
  - Cloud Computing
  - NIST Cybersecurity Framework 2.0
  - National Cybersecurity Strategy
- Emerging Cyber Risks
  - Artificial Intelligence
  - Quantum Computing
- ABA and other Resources
- Q&A

John Carlson
Senior Vice President, Cybersecurity Regulation and Resilience

- Prior Private Sector Leadership
  - Global Financial Services Industry Lead Security Assurance, Amazon Web Services
  - Chief of Staff, FS-ISAC
  - Executive Vice President, BITS/Financial Services Roundtable
  - Managing Director of Operational Risk, Morgan Stanley
- Prior Public Sector Leadership
  - Director of Bank Technology, OCC
  - Budget Analyst, U.S. Office of Management and Budget
  - Senior Analyst, Federal Reserve Bank of Boston
- MPP, Kennedy School of Government at Harvard University
- BA, University of Maryland

Top Cyber Issues: Adversaries & Motivations

- Adversaries:
  - Organized criminal enterprises
  - Nation-states
    - China
    - Russia
    - Iran
    - North Korea
  - Trusted insiders

- Motivations
  - Financial gain
  - Ideological reasons
  - Espionage
  - Terrorism/Sabotage
  - Warfare

Cyber Attacks

- Third-party attacks due to reliance on a myriad of providers and suppliers
- Zero-day vulnerability exploits due to the increasing attack surface caused by digitization of the financial sector
- Ransomware attacks with demands for payment in cryptocurrencies
- Social engineering (e.g., phishing, business email compromise)
- Distributed denial of service (DDoS) attacks
- Breaches

2024 Verizon Breach Report

- All Industries
  - 68% of all breaches involve human element (down 6% from 2023)
  - External actors still the top catalyst for breaches at 65%. But internal actors (at 35%) increased from 20% in 2023
  - 28% of breaches involved errors, while 15% of breaches involved a 3rd party (including software vulns)
  - Most popular methods used by external actors: stolen credentials, phishing, exploit vulnerabilities
  - Roughly one-third of all breaches involved ransomware or some other extortion technique.
    - Roughly 23% Ransomware, roughly 9% pure extortion
  - Roughly 92% of attacks observed last year were financially motivated, while espionage as a motive increased from 5% to 7%
- Finance and Insurance:
  - System intrusion has overtaken miscellaneous errors and basic web application attacks as the primary threat in Financial and Insurance this year, indicating a shift toward more complex attacks

Report: https://www.verizon.com/business/resources/reports/dbir/2024/summary-of-findings/

2023 FBI Internet Crime Compliant Center (IC3)

- IC3 received a record number of complaints from the American public: 880,418 complaints, with potential losses exceeding $12.5 billion.
  - 10% increase in complaints, representing a 22% increase in losses compared to 2022.
- Most losses reported to the IC3 are the result of frauds and scams.
  - Complainants report a wide variety of payment methods in these scams, such as cash and gold shipments, wire transfers, prepaid and gift cards, and cryptocurrency ATMs.
- Top victim losses (2023):
  - Investment fraud losses rose from $3.31 billion in 2022 to $4.57 billion in 2023, a 38% increase.
    - Investment fraud with a reference to cryptocurrency rose from $2.57 billion in 2022 to $3.96 billion in 2023, an increase of 53%
  - 2,825 complaints identified as ransomware with adjusted losses of more than $59.6 million
  - Business Email Compromise (BEC): 21,489 BEC complaints with adjusted losses over $2.9 billion
  - Tech Support: over $924 million with 37,560 complaints received
  - Personal data breach: over $744 million
  - Confidence/Romance scam: over $652 million
  - Real Estate: over $145 million
  - Non-payment/non-delivery: over $309 million
  - Check Card/Check Fraud: over $173 million
  - Government impersonation: over $394 million with 14,190 complaints received
  - ID theft: over $126 million

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

Federal Cyber-Related Regulatory Requirements

- Gramm-Leach-Bliley (GLBA) Safeguards Rule
- FFIEC Information Technology Booklets (e.g., Information Security, Outsourcing Technology Services, Architecture, Infrastructure and Operations, Business Continuity Management
- Third party risk management - Guidance on Third-Party Risk Management (FDIC, FRB, OCC)
- Incident notification, disclosures, and governance:
  - Computer Security Incident Notification Rule (FDIC/FRB/OCC)
  - Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure, proposed amendments to Reg S-P, Reg SCI and Exchange Act (SEC)
  - Federal House Administration (FHA) notification requirements for mortgage providers
  - Cyber Incident Reporting for Critical Infrastructure Act of 2022 (proposed by DHS/CISA)

Third Party Risk Management

- FDIC, FRB, OCC Rule on Third Party Risk Management (June 2023)
  - Describes principles and considerations for banking organizations' risk management of third-party relationships
  - Covers risk management practices for the stages in the life cycle of third-party relationships: planning, due diligence and third-party selection, contract negotiation, ongoing monitoring, and termination
  - Includes illustrative examples to help banking organizations, particularly community banks, align their risk management practices with the nature and risk profile of their third-party relationships
  - Replaces each agency's existing general third-party guidance and promotes consistency in the agencies' supervisory approaches toward third-party risk management
- Financial Stability Board consultation on third-party risk management and oversight for critical providers
- US Treasury Cloud Report and Workstreams

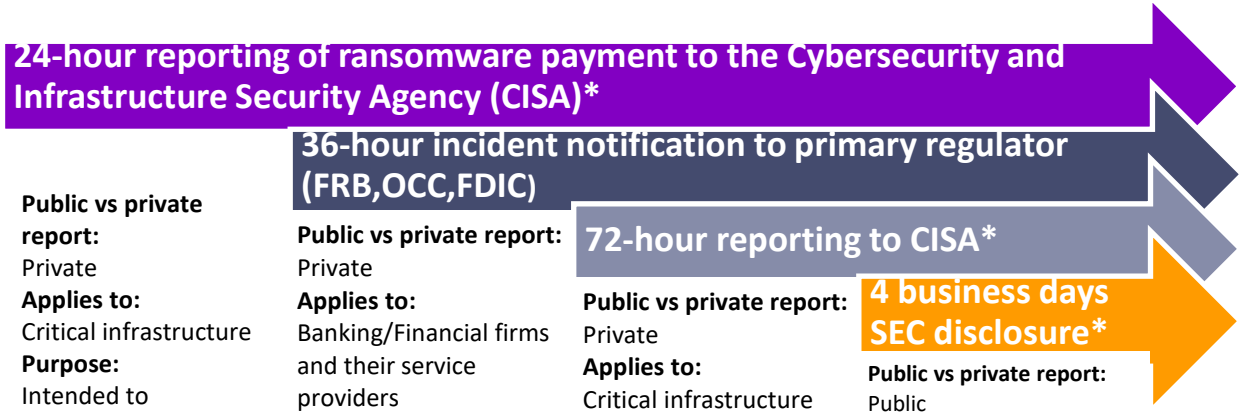
DHS/CISA Incident Notification Proposal (1/2)

- Applies to all regulated FIs already required to report cybersecurity incidents to their respective primary Federal regulator
  - Includes examples of incidents that do or do not qualify as "substantial" cyber incidents
  - Reports submitted through the web-based CIRCIA Incident Reporting Form
  - Exemption from FOIA and other public disclosures
- Lays out submission timelines:
  - Covered Cyber Incidents Report: **no later than 72 hours** after the covered entity reasonably believes a covered cyber incident has occurred
  - Ransomware Payment: **not less than 24 hours**
  - Supplemental Reports: **“Promptly**” if **“substantial new or different information”** becomes available, **or if the covered entity pays a ransom after submitting a covered cyber incidents report**

DHS/CISA Incident Notification Proposal (2/2)

- Includes a long list of required information for covered cyber incident reports, ransom payment reports, and supplementary reports
- Other:
  - Third party reporting procedures and requirements
  - Data and records preservation requirements
  - Request for information and subpoena procedures
  - Civil enforcement of subpoenas
- ABA collaborated with other associations on a comment letter: https://www.aba.com/advocacy/policy-analysis/joint-ltr-dhs-cyber-circia-proposal

Challenge: Different Timelines for Cyber Incident Reporting



Public vs private report:
Private
Applies to:
Critical infrastructure
Purpose:
Intended to encourage coordination with law enforcement; support investigations
Info requirements:
Some details around the payment/extortion scheme

*awaiting final rule

Public vs private report:
Private
Applies to:
Banking/Financial firms and their service providers
Purpose:
Intended to provide early warning to regulators
Info requirements:
Very little detail required; phone call or email

Public vs private report:
Private
Applies to:
Critical infrastructure
Purpose:
Intended to improve detection and analysis of threats across industries; improve early warning
Info requirements:
Will require details on tactics, techniques, other forensics

Public vs private report:
Public
Applies to:
All publicly traded companies
Purpose:
Intended to ensure investors have timely information on security of firms and improve firms' security practices
Info requirements:
Details on incident discovery, nature and scope, whether it is ongoing or remediated, and whether data was stolen, altered, accessed, used, etc.

Key Advocacy Points on Notification Requirements

- Harmonize!
  - Government agencies and regulators should work together to develop a common reporting form that would be useful for all government entities requiring incident reporting.
  - Advance common standards for incident reporting among US and foreign regulators.
- Cyber incident info should be tightly linked with an actionable purpose
  - Regulations should be designed to protect against cyberthreats, not to impose intrusive administrative burdens that also create undue enforcement and litigation risks.
- Reportable cyber incidents should include only incidents of a particularly elevated severity and malicious intent that cause material harm to the critical infrastructure entity at the enterprise level.
- Create a staggered reporting requirement composed of an initial, high-level notification of the immediately known details of the incident within 72 hours containing actionable information for CISA to monitor, and supplemental material updates on an ongoing basis to fulfill the enumerated statutory requirement.
  - Supplemental reports should be voluntarily submitted upon the determination by the covered entity that circumstances surrounding the incident have materially changed.
- Include a law enforcement and cybersecurity agency exception

Other Significant Developments

- Unique Public-Private Sector Collaboration:
  - Cloud Computing: US Treasury Report and FSSCC-FBIIC Cloud Workstreams
  - AI: US Treasury paper and proposed AI workstreams
- NIST Cybersecurity Framework 2.0
- Biden Administration National Cybersecurity Strategy
- Biden Administration Executive Order on AI

US Treasury Cloud Report (Feb 2023)

- Explores how the use of cloud services may affect the sector's operational resilience.
- Provides an overview of cloud services, how financial institutions rely on cloud service provider (CSPs), and the advantages of using CSPs.
- Lays out key drivers
  - Faster development and scaling of new applications and services using cloud infrastructure and tools;
  - Competitive challenges and customer demands for digital financial products and partner with fintechs;
  - Increased resilience to physical and cyber incidents;
  - The opportunity to retire legacy technology and reduce costs; and
  - Expand IT infrastructure to support remote workers and customers' use of digital financial services which have been hastened by the COVID-19 pandemic.

US Treasury Cloud Report (cont'd)

- Lays out key challenges financial institutions face:
  - Insufficient transparency to support due diligence and monitoring by financial institutions;
  - Gaps in human capital and tools to securely deploy cloud services;
  - Exposure to potential operational incidents, including those originating at a CSP;
  - Potential impact of market concentration in cloud service offerings on the sector's resilience;
  - Dynamics in contract negotiations given market concentration; and
  - International landscape and regulatory fragmentation.

US Treasury Cloud Report (cont'd)

- Action plan:
  - Establish "Cloud Services Steering Group" with participation of federal financial regulators to promote closer domestic cooperation among U.S. regulators;
  - Facilitate further engagement between the financial sector and CSP
  - Conduct tabletop exercises with industry;
  - Review sector-wide incident protocols in light of growing reliance on cloud services;
  - Consider ways to appropriately measure cloud service dependencies across the sector and assessing systemic concentration and related risks on a sector-wide basis;
  - Identify ways to foster effective risk management practices in the financial services industry;
  - Continue to support the development of relevant standards and international policies at the G7, the Financial Stability Board, and the international financial standard-setting bodies; and
  - Explore ways to increase international collaboration and coordination on financial regulatory issues arising from cloud services.

July 2024: Cloud Deliverables

- Common lexicon that may be used by financial institutions and regulators in discussions regarding cloud.
- Enhanced information sharing and coordination for examination of cloud service providers.
- Assessed existing authorities for cloud service provider (CSP) oversight.
- Established best practices for third-party risk associated with cloud service providers, outsourcing, and due diligence processes to increase transparency.
- Provided a roadmap for institutions considering comprehensive or hybrid cloud adoption strategies including an update to the Financial Sector's Cloud Profile.
- Improved transparency and monitoring of cloud services for better "security by design."
- https://home.treasury.gov/news/press-releases/jy2467

NIST Cybersecurity Framework Update (CSF 2.0)

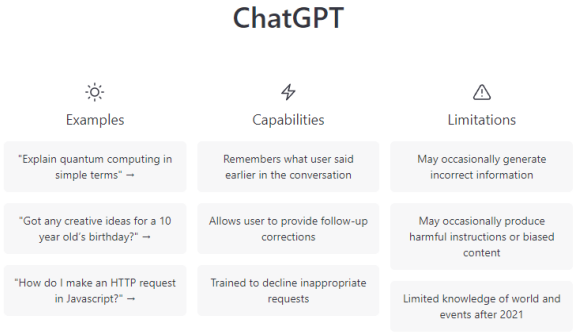
- National Institute for Standards and Technology (NIST) released updated Cybersecurity Framework 2.0 in 2024
  - Added new “Govern” function and expanded references to third party risk management.
- Cyber Risk Institute (CRI) Profile aligned to CSF 2.0.
- OCC released in 2023 the Cybersecurity Supervision Work Program (CSW) which includes a specific call out of the CRI Profile.
  - The CSW maps the procedures to existing supervisory guidance and industry cybersecurity frameworks including Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool, the Center for Internet Security’s Critical Security Controls, and the CRI Profile.
  - The CSW is structured according to the five NIST-CSF functions—Identify, Protect, Detect, Respond, and Recover—and the related categories and subcategories.

Biden Admin National Cybersecurity Strategy

- Released March 2023; Implementation Plan Released July 2023
  - Outlines timetable and lead agencies
- Key Elements:
  - Promote development of secure software products and services
  - Reduce compliance burden through harmonization of regulations
  - Engage/oversee cloud service providers and other essential third-party services
  - Disrupt and dismantle threat actors
  - Increase the capacity of international coalitions and partnerships to counter threats to the digital ecosystem
  - Invest in the foundation of the Internet
  - Explore a Federal cyber insurance backdrop

Artificial Intelligence – Friend or Foe?

- Ask ChatGPT “What risk does AI pose to humanity?”
  - Job displacement
  - Bias and discrimination
  - Misuse – misinformation, cyberattacks, committing fraud
  - Privacy and Security compromises
  - Autonomous weapons
  - Singularity

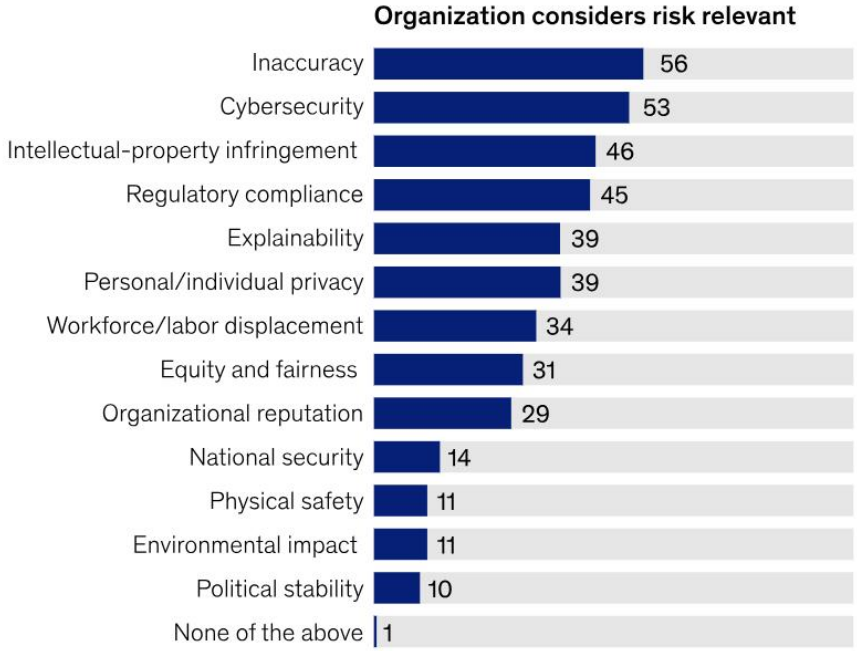


https://chat.openai.com/chat

- In banking focus is on bias, cyberattacks and security compromises
  - Bias is already a concern in algorithms being used
  - Cyberattacks could be enabled by AI improved algorithms breaking encryption
  - Automation of security compromises - imagine an AI with access to someone’s PII

Emerging Risk: Artificial Intelligence

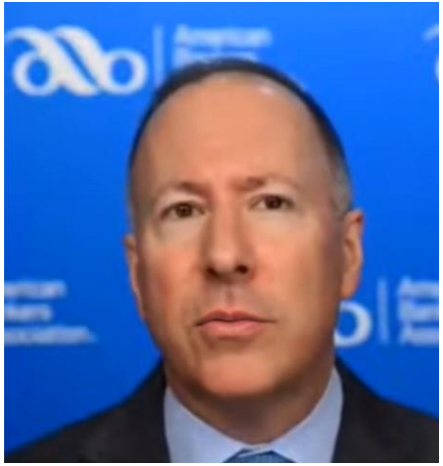
Inaccuracy and cybersecurity are the most-cited risks of generative AI adoption



Source: The state of AI in 2023: Generative AI's breakout year [McKinsey Global Survey](#) (Aug. 2023)

Advances in AI Deep Fake Technologies

Video Source of Screen Grab



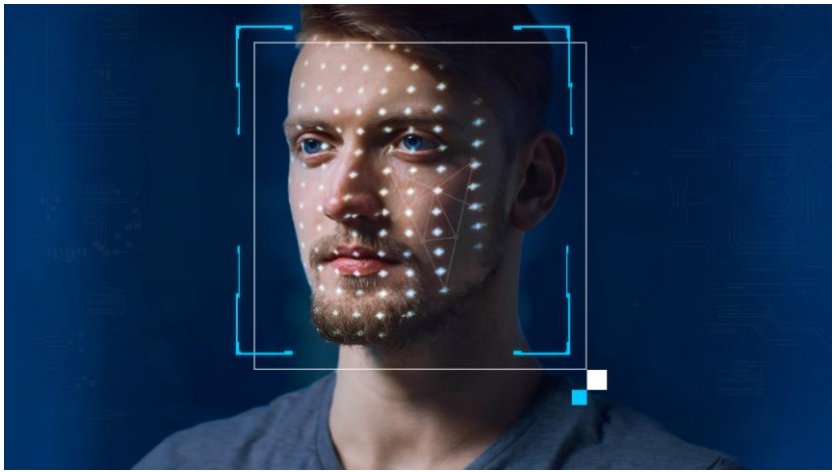
Use the image and copy the voice - turns into something nefarious

Or, something funny

Deepfake Detection Systems

Some companies that are offer services to detect deepfakes

- Pindrop
- Omilia
- Google SynthID
- Intel FakeCatcher
- Microsoft Video Authenticator
- Reality Defender
- Sensity
- Sentinel
- WeVerify Deepfake Detector
- Udentify



Source: Intel, Deepfake Detection

Steps Banks Could use to Verify Customer Legitimacy

Deepfake and synthetic media technology is becoming increasingly advanced. With the rise of quality, it has become harder for individuals to tell real from fake.

There may be noticeable inconsistencies in the deepfake that will give it away, some being:

- Unnatural eye movements
- Lack of emotion
- Lips not always synchronized with the audio
- Noticeable jumps in the video
- Blurring around the edges of a person's face

Some other tactics that can be used include checking for inconsistencies with previous recordings or photographs of the person in question.

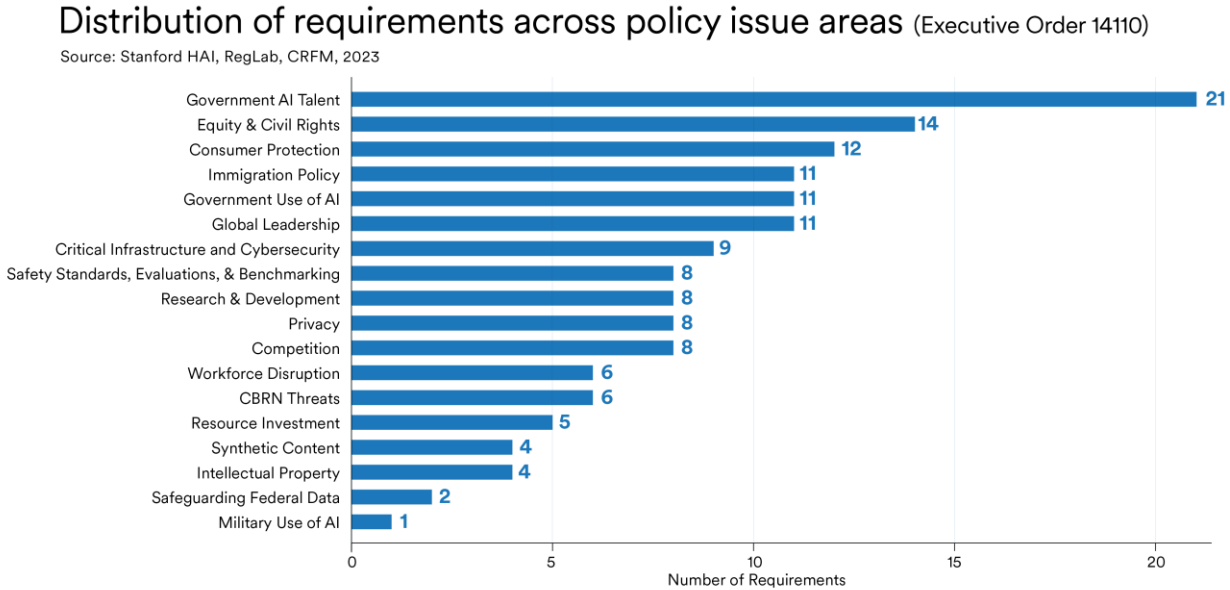
- Do their mannerisms, facial expressions, and voice match up?
- Asking the customer to turn their face to the left and right is also a good option if you suspect the live video to be a deepfake.

Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence

- Directs numerous federal agencies to review and draft new regulations on the use of AI across multiple sectors
  - Builds on previous Administration efforts including the "Blueprint for an AI Bill of Rights", AI Risk Management Framework, and AI Cyber Challenge.
- Advances numerous policy objectives, including:
  - promoting safety and security
  - managing risks
  - promoting responsible innovation and competition
  - supporting American workers
  - advancing equity and civil rights
  - protecting privacy and civil liberties
  - advancing US global leadership on AI
- Establishes several councils and advisory councils to coordinate efforts across the government and to engage the private sector

Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence:

- Addressing AI safety, security, and reliability concerns is a clear focus.
- Requirements outlined in Section 4 (Safety) that are related to safety standards, evaluations, and benchmarking; critical infrastructure and cybersecurity



Impact of EO on AI on Banks (1/2)

- Cyber
  - Requires the U.S. Department of the Treasury to report how the banking sector can manage cyber risks involved in the use of AI technologies
    - Published in March 2024; includes current uses cases, best practices recommendations, challenges and opportunities (See appendix)

- Third Party Risk Management
  - Signals greater Federal oversight of AI and cloud service providers
  - Directs regulatory agencies to clarify due diligence responsibilities for ongoing monitoring of third-party AI services

- Anti-Discrimination in Lending and Advertising
  - Directs the CFPB, HUD, and FHFA to combat AI-enabled discrimination in access to credit, housing, and in other real estate-related transactions

Impact of EO on AI on Bank (2/2)

- Privacy
  - Urges independent regulatory agencies to emphasize or clarify AI's threats to privacy
- Fraud, Spam and Synthetic Content
  - Encourages independent regulatory agencies' use of existing authorities to protect consumers from fraud through enhanced detection and authentication
- Workforce
  - Requires Secretary of Labor to develop and publish principles and best practices for employers that could be used to mitigate AI's potential harms to employees' wellbeing and maximize its potential benefits
- Testing
  - Requires companies building the most advanced AI systems to perform safety tests and notify the government of the results before rolling out products

US Treasury Report on AI and Cyber (1/4)

- Defines AI as “a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.”

US Treasury Report on AI and Cyber (2/4)

- Outlines ways cyber threat actors can use AI, including social engineering, malware/code generation, vulnerability discovery, and disinformation
- Notes ability of bad actors to use AI to impersonate individuals in ways that were previously much more difficult" (e.g., deepfakes, synthetic identities)
- Emphasizes importance of third-party risk management and data integrity
- Offers a model of responsible AI governance
- Describes existing regulatory requirements for model risk management, technology risk management, data management, compliance and consumer/investor protection, and third-party risk management

US Treasury Report on AI and Cyber (3/4)

- Best Practices for Managing AI-specific Cybersecurity Risks
  - Situate AI risk within enterprise risk management programs
  - Develop and implement an AI framework
  - Integrate risk management functions for AI
  - Evolve the chief data officer (CDO) role and map the data supply chain
  - Ask the right questions of vendors
  - Survey NIST's Cybersecurity Framework for AI opportunities
  - Implement risk-tiered multifactor authentication mechanisms
  - Pick the right tool for the job and risk tolerance.

US Treasury Report on AI and Cyber (4/4)

- Next Steps and Opportunities
  - Develop for common AI lexicon
  - Address growing capability gap between the largest and smallest FIs
  - Narrow the fraud data divide
  - Clarify how AI will be regulated in the future
  - Expand the NIST AI Risk Management Framework
  - Develop best practices for data supply chain mapping disclosures (aka “nutrition labels”)
  - Decipher explainability for black box AI solutions
  - Address gaps in human capital
  - Untangle digital identity solutions
  - Coordinate with international authorities

Summary: https://bankingjournal.aba.com/2024/04/treasury-ai-fueled-cyber-threats-bring-new-challenges/

Financial Sector R&D Paper on AI

- ABA led effort by the Financial Services Sector Coordinating Council (FSSCC) to develop a paper that examines the current and anticipated use cases of cybersecurity and fraud AI solutions within the sector
- Lays out considerations for navigating the evolving landscape:
  - Enhanced cybersecurity measures
  - Advanced fraud detection mechanisms
  - Prepare for sophisticated AI-enabled attacks, such as complex phishing and social engineering tactics
  - Deploy robust risk management strategies
  - Collaborate to develop standardized strategies for managing AI-related risk
  - Invest in human expertise
  - Urge regulators to apply flexible risk-based approaches
- US Treasury incorporated the FSSCC paper in the appendix of its March 2024 report on AI and cyber

ABA advocates for a principles-based policy approach

01 Develop a common lexicon and understanding of the AI ecosystem

02 Take an industry-based approach to minimize the impact to banks that already have a history of complying with laws and regulations related to AI

03 Regulations should be technology-neutral, risk-based and tailored to particular use cases

Emerging Risk: Post Quantum Computing (PQC) Encryption

- Massive investments being made in quantum computers
- FIs rely on encryption to safeguard information including payments
- Potential to break standard encryption algorithms within next 5-10 years
  - Concerns with adversaries siphoning encrypted data to decrypt later
- Organizations must transition to quantum-resistant encryption algorithms that NIST is developing
  - Some similarities to Y2K
- Significant challenges:
  - Inventorying encryption in software and hardware
  - Third party risk management
  - Testing
  - Business continuity planning

PQC: Public Sector Efforts

- The US Government launched multi-pronged strategy to address the risk, develop standards and ensure that the USG is prepared.
  - Important example of public-private sector collaboration
- Standards: NIST Post-Quantum Cryptography Standards
  - https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization
  - Anticipated release Summer 2024
- Biden Administration National Security Memorandum outlining the Administration's plan for US Government Agencies to address the risks posed by quantum computers to America's cybersecurity (May 2022)
- Passage of "Quantum Computing Cybersecurity Preparedness Act" (Dec 2022)
  - Directs OMB to: a) prioritize the acquisition and migration of federal agencies' information technology to post-quantum cryptography, b) create guidance for federal agencies to assess critical systems one year after NIST issues planned post-quantum cryptography standards.
- Guidance:
  - G-7 Cyber Expert Group (expected in late September 2024)
  - US federal banking agencies have not issued any specific guidance yet.

PQC: Private Sector Efforts

- Association Awareness Efforts
  - American Bankers Association (ABA)
  - Financial Services Sector Coordinating Council (FSSCC)
  - Financial Services Information Sharing and Analysis Center (FS-ISAC)
    - FS-ISAC: Preparing for a Post-Quantum World by Managing Cryptographic Risk: https://www.fsisac.com/knowledge/pqc
    - Goal: Crypto agility
- Individual financial association efforts

ABA Cybersecurity Efforts

- Cyber Committees
- Leadership in the Financial Services Sector Coordinating Council
  - Cloud workstreams
  - “Hamilton” series cyber exercises (with US Treasury)
  - R&D priorities and focus on AI and quantum computing
  - Support for .bank, Sheltered Harbor and Cyber Risk Institute (CRI)
- Consumer education - #BanksNeverAskThat and the ABA Foundation
- ABA/Oliver Wyman Paper on Trusted Digital Identities (https://www.aba.com/news-research/analysis-guides/the-growing-significance-of-trusted-digital-identities-in-us-financial-services)
- ABA Risk Management School and Courses on Cyber, Business Continuity, and Third-Party Risk
- Conferences on risk management, compliance and financial crimes
- Engagement with financial regulators (e.g., comment letters) and law enforcement

ABA AI Efforts and Working Groups

- ABA AI Working Group
  - ABA Cyber and Fraud AI Subgroup
- Enterprise Privacy and Data Governance Working Group
- 1033/Data Aggregation Working Group
- Model Risk Management Working Group
- Third Party Risk Management Working Group

- Note: July 23, 2024: ABA Statement for the record on AI that provides a good overview of how banks use AI: https://www.aba.com/advocacy/policy-analysis/sfr-ai-innovation-explored

ABA Resources for Cyber Security

- ABA Crisis Communication Toolkit https://www.aba.com/news-research/analysis-guides/crisis-communications-toolkit
- ABA's Social Media Toolkit https://www.aba.com/news-research/analysis-guides/social-media-toolkit
- ABA (anti) Ransomware Toolkit: https://aba.com/ransomware
- SolarWinds Resource Page: https://www.aba.com/banking-topics/risk-management/incident-response/solarwinds-orion-code-compromise
- Financial Services Sector Cybersecurity Profile: https://cyberriskinstitute.org/the-profile/
- Tips on Safeguarding Your Bank and Customers from Business E-mail Compromise (BEC) Scams
- Principles for Strong Bank-Core Provider Relationships
- .bank https://www.register.bank/

More at aba.com/Cyber

US Government Resources

DHS Cybersecurity and Infrastructure Security (CISA) resources:

- https://cisa.gov/cybersecurity
- https://cisa.gov/stopransomware
- https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- https://www.cisa.gov/resources-tools/services/web-application-scanning

NIST:

- https://www.nist.gov/itl/smallbusinesscyber
- NIST DRAFT Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profi le Rev. 3.0 Special Publication (SP) 800-61 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.ipd.pd

US Secret Service Preparing for a Cyber Incident:

- https://www.secretservice.gov/investigation/Preparing-for-a-Cyber-Incident

FBI IC3:

- https://www.ic3.gov/

FinCEN:

- Rapid Response Program (RRP): https://www.fincen.gov/sites/default/files/shared/RRP%20Fact%20Sheet%20Notice%20FINAL%20508.pdf

Federal Reserve Bank Synthetic ID Toolkit

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

QUESTIONS (now or later)?

John Carlson, Senior Vice President for Cybersecurity Regulation and Resilience
Email: Jcarlson@aba.com
Tel: 202.663.5589

Maryland Banking School

College Park, MD

2024

Roadmap

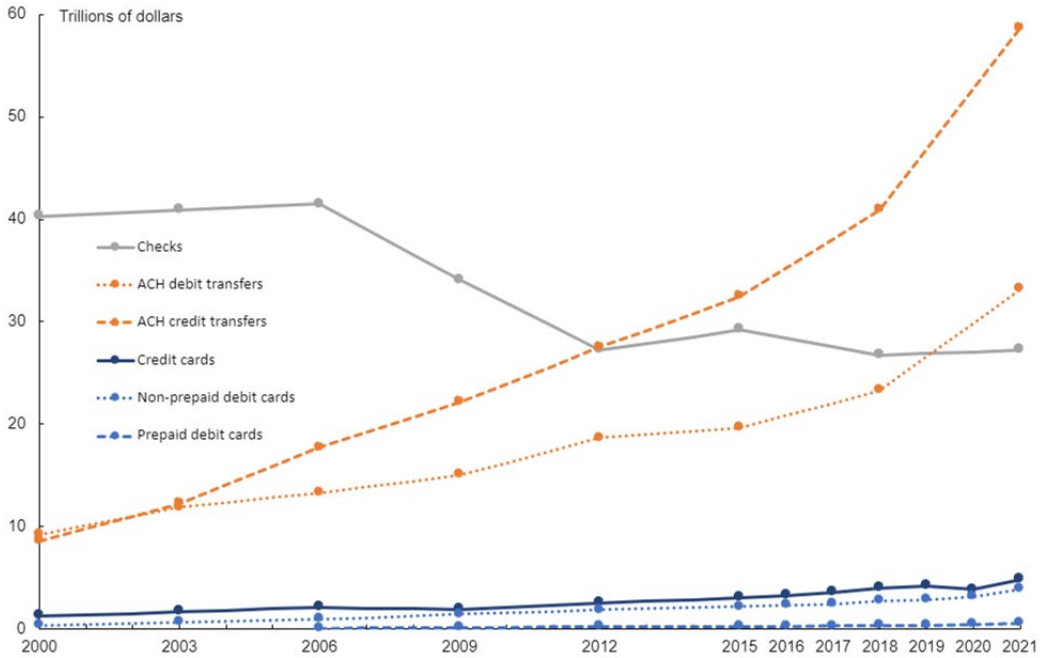
- Federal Reserve Payments Study
- TCH Real Time Payments Live Since 2017
- FedNow Launched July 20, 2023
- Zelle
- Board Proposal for 22/7/365 Fedwire….and ACH
- Coin Circulation
- Reducing Paper Checks

Speaker

- Steve Kenneally, SP, Payments American Bankers Association
- Legacy Systems
  - Checks, wires, ACH, cards, coins and paper money
- New Systems
  - FedNow, TCH RTP, Zelle, Stablecoins, CBDC, and cryptocurrency
- Industry Groups
  - ABA's Payments Committees, Nacha Payments Innovation Alliance Consumer Advisory Board Member, TCH RTP Advisory Committee, IBFed Payments Work Group, Faster Payments Council

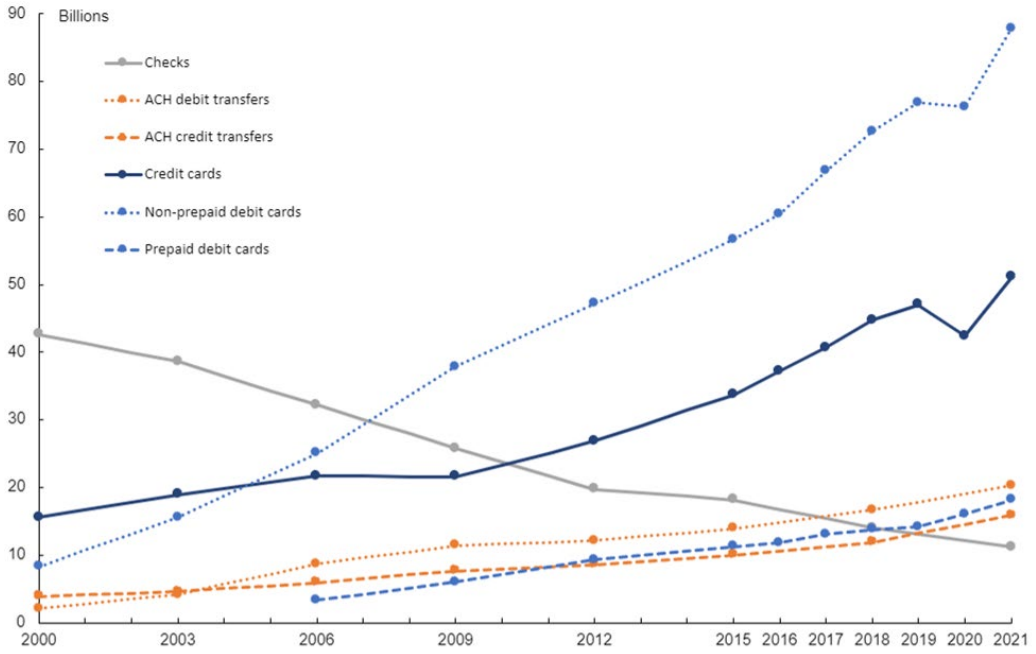
Trends in non-cash payments by dollar value 2000-2021

Federal Reserve Survey



Trends in non-cash payments by transaction 2000-2021

Federal Reserve Survey



The Clearing House Real Time Payments Network

Overview

- Launched in November 2017 and currently implemented by The Clearing House (TCH) with 655+ banks live
- Allows US banks to offer 24/7/365 real-time payment services capped at $1 million per transaction
- Currently reaches over 60% of US transaction accounts, with a goal of providing every financial institution in the US an easy way to access the RTP network by 2020

Process

- Available to all federally-insured US depository institutions
- Can be used for consumer and business payments
- Provides sending, clearing, and settlement capabilities
- Works in the background of a financial institution's customer-facing systems for services like bill payment and cash management

Key Issues

- Competes with FedNow
- It is questionable whether TCH RTP and FedNow will become interoperable
- TCH RTP requires a separate prefunded account that does not pay interest or count towards capital reserves
- TCH and member banks have expressed a lack of support for the Fed's real-time payments system, which is currently in development

Sources: PR Newswire, PYMNTS.com, The Clearing House, Forbes.

FedNow

Overview

- Developed by the Federal Reserve
- Allows banks in the US to offer 24/7/365 real-time payment services
- Launched July 2023

Process

- Enables all banks to provide real-time payments through their master accounts held at the Federal Reserve
- Eases delays and built-up financial obligations between banks that could present risks to the financial system
- Supports transfers of up to $500,000 at bank discretion
- Separately exploring extending Fedwire and National Settlement Service to 24/7/365!!!!!

Key Issues

- Interoperability
- Chartered FI Access
- Liquidity Concerns
- Parity with TCH RTP
- Core Service Providers
- Equitable Pricing
- ISO 20022
- Fedwire and NSS 24/7/365

Sources: Tech Crunch

THE FEDERAL RESERVE
FRBservices.org

Announcing Organizations Certified as Ready for the FedNow® Service

	JPMorgan Chase	$3.3T
	Wells Fargo Bank, N.A.	$1.7T
	U.S. Bank	$590B
	BNY Mellon	$32B
UFS / Fiserv	Nicolet National Bank	$8.2B
FIS	1st Source Bank	$8B
Fiserv	Peoples Bank	$7.2B
Fiserv	Salem Five Bank	$6.7B
	First Internet Bank of Indiana	$4.7B
FIS	Avidia Bank	$2.6B
	Quad City Bank & Trust	$2.5B
Jack Henry	Bryant Bank	$2.4B
	U.S. Century Bank	$2.2B
	Malaga Bank	$1.5B
OPN	North American Banking Co	$1.2B
FPS Gold	1st Bank Yuma	$600M
Fiserv	Mediapolis Savings Bank	$235M
	Buffalo Federal Bank	$183M
Jack Henry	Bridge Community Bank	$125M
	Global Innovations Bank	$50M

Bankers' Banks

- Atlantic Community Bankers Bank
- Bankers' Bank of the West
- Community Bankers' Bank
- PCBB
- The Bankers Bank
- United Bankers' Bank

Credit Unions

- Alloya Corporate Federal Credit Union
- Catalyst Corporate Federal Credit Union
- Consumers Cooperative Credit Union
- Corporate America Credit Union
- Corporate One Federal Credit Union
- Eastern Corporate Federal Credit Union
- HawaiiUSA Federal Credit Union
- Michigan Schools & Government Credit Union
- Millennium Corporate Credit Union
- Pima Federal Credit Union
- Star One Credit Union
- Veridian Credit Union
- Vizo Financial Corporate Credit Union

Service Providers

- ACI Worldwide Corp.
- Alacriti
- Aptys Solutions
- ECS Fin Inc.
- Finastra
- Finzly
- FIS
- Fiserv Solutions, LLC
- FPS GOLD
- Jack Henry
- Juniper Payments, a PSCU Company
- Open Payment Network
- Pidgin, Inc.
- Temenos
- Vertifi Software, LLC

Misc

- U.S. Department of the Treasury's Bureau of the Fiscal Service
- Adyen - International Acquiring Bank

Zelle

Overview

- Launched in June 2017 and currently implemented by more than 1,800 banks and credit unions
- Customer facing P2P credit push
- Owned by Early Warning Services, a consortium of large banks

Process

- Available to all federally-insured US depository institutions
- Can be used for consumer and business payments, but primarily used for P2P
- Provides a directory service that links bank accounts to mobile phone numbers and email addresses
- Payments settle through ACH, not through Zelle.

Key Issues

- Fraudulently induced authorized transactions not covered by Regulation E
- Ownership group
- Linked to fraud in media coverage

Sources: PR Newswire, PYMNTS.com, The Clearing House, Forbes.

FedNow/TCH RTP/Zelle

	FedNow	The Clearing House RTP	Zelle
Operator	Federal Reserve	The Clearing House	Early Warning Services
Operating Hours	24/7/365	24/7/365	24/7/365
Function	Non-customer facing bank to bank system	Non-customer facing bank to bank system	Customer-facing directory-based P2P service
Launch Date	July 2023	2017	2017
Transaction Speed	Seconds	Seconds	Seconds
Payment Type	Credit Push Only	Credit Push Only	Credit Push Only
Transaction Limits	$500,000 $100,000 Default Limit FIs can adjust the limits	$1,000,000 FIs can adjust the limits downward	Set by individual FIs
Settlement Type	Real Time Gross Settlement from the FI master account	Real Time Gross Settlement from within a prefunded account held at the FRB-NY	-ACH or TCH RTP in limited circumstances -Receiving FI must credit customer account immediately with the funding transaction to follow
Reversals	No, all payments are final	No, all payments are final	All payments are final with a small number of exceptions
If Settlement Account Balance Is Zero	Payment will be processed and master account will go into overdraft	Payment will not be processed	Payment will not be processed if customer account balance is zero
Cross-Border	Not at this time	Pilot project with SWIFT and European Banking Association CLEARING	Sender and Receiver FIs must be based in the U.S.

Board Proposal for 22/7/365 Fedwire and NSS

- Fedwire would operate 22/7/365
  - FIs can opt in or out
  - FIs opting out would post wires on next business day
  - Implementation date no sooner than March 2027
  - Difficult to project volumes to determine if it makes sense to opt in
- NSS
  - Enabling NSS enables ACH operations to run seven days a week
  - Nacha would have to change rules
  - More difficult for FIs to opt out for competitive reasons

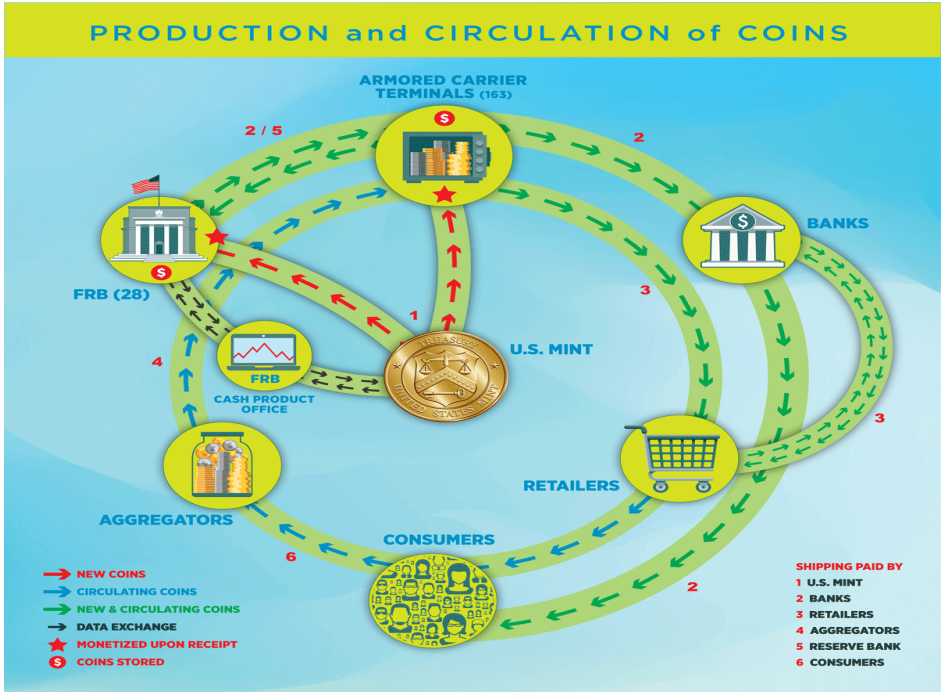
Board Proposal for 22/7/365 Fedwire and NSS

- What would operating Fedwire 22/7/365 mean for your bank?
  - What would it cost to opt in? Staffing?
  - What are the downsides of opting out?
- What would 22/7/365 ACH operations mean for you bank?
  - What would it cost to opt in? Staffing?
  - What are the competitive downsides of opting out? Could your bank opt out?
- Comments due September 6, 2024

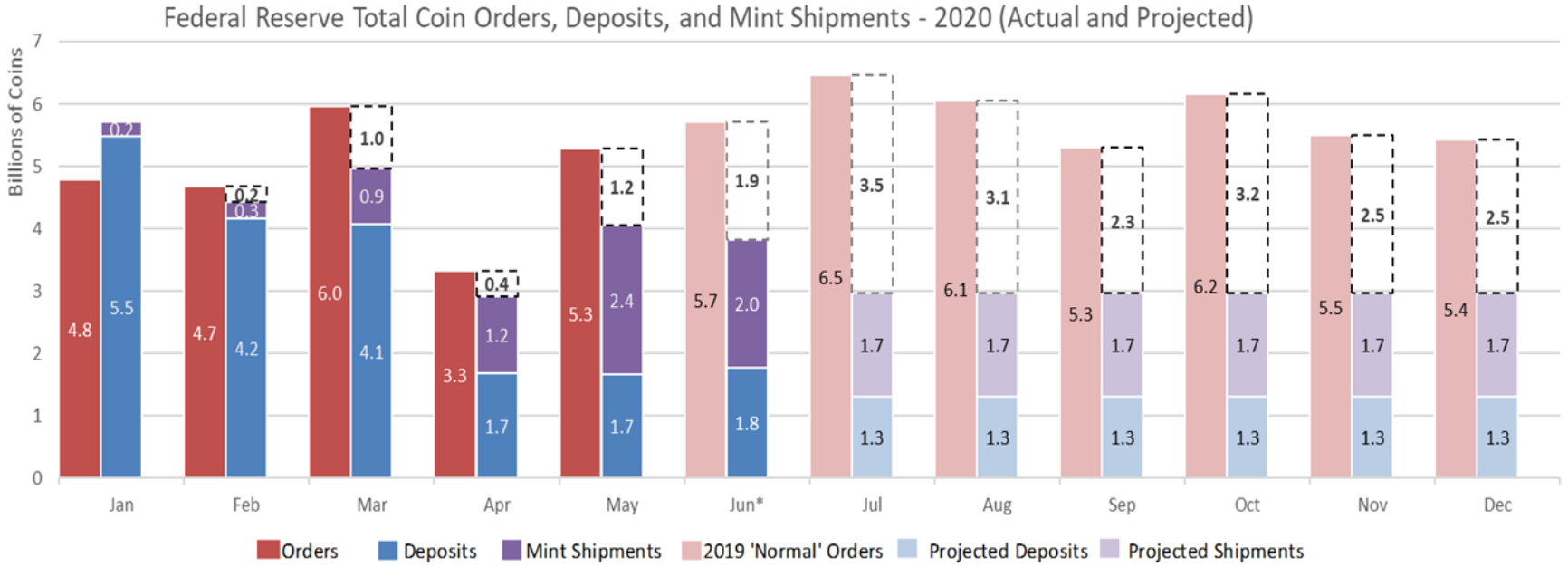
Circulation of Coin in Normal Times

U.S. COIN TASK FORCE

#getcoinmoving



US Coin Supply and Demand



*Jun-Dec Orders use 2019 FRB monthly coin order volume as a proxy for 'normal' coin demand in place of actual 2020 orders, which are limited by coin allocation

Coin Circulation Tools

- Encourage consumers to use exact change
- Encourage consumers to “cash out” coins at banks and coin aggregators.
  - Coin drives for employees.
  - Rewards for customers.
- Round up/round down deposits (Banks).
- Round up/round down purchases (Merchants).

American Bankers Association

Steve Kenneally
Senior Vice President, Payments
American Bankers Association
skenneally@aba.com
202-663-5147

Building Success. Together.

Fraud Operations and Response

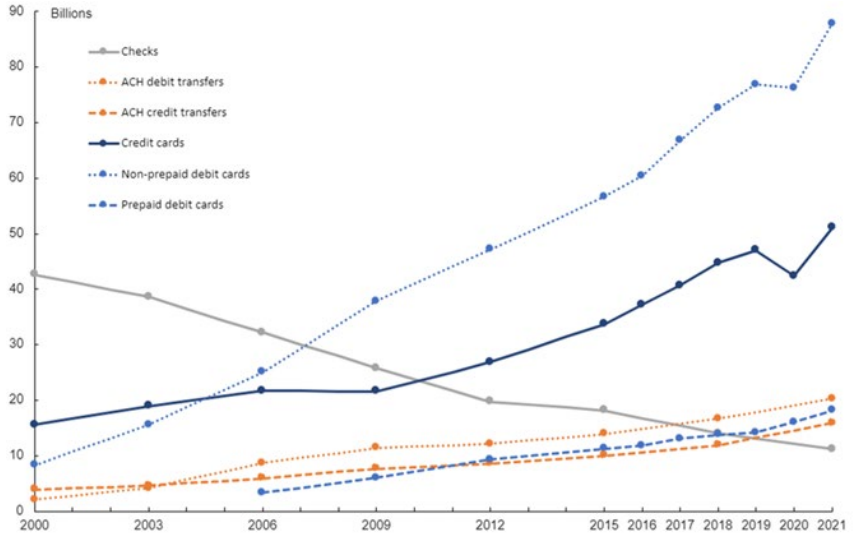
Agenda

1. Fraud Risks and Actions
2. Fraud Ecosystem
3. Fraud Prevention and Detection Operations
4. Filing with Law Enforcement
5. Questions

FRAUD RISKS AND ACTIONS

FRAUD RISKS STATISTICS

Transactions Growth



$3B in business email compromise fraud. Federal Bureau of Investigation, 2024

Check fraud rose from 65% of payments fraud to 80% of payments fraud. AFP 2024 Payments Fraud. NACHA

Nearly 60% of banks, fintechs and credit unions have lost over $500K USD in direct fraud losses over 2023. *Alloy, State of Fraud Benchmark Report*

Payment fraud increased 22% from 2022 to 2023. *Nice Actimize*

Impersonation scams are on the rise. $618M USD losses were reported for consumers scammed by government impersonation fraud. Federal Trade Commission

More than 80% of financial institutions report spending more on fraud mitigation. Federal Reserve of Atlanta

Current and Emerging Fraud Risks

Check Fraud

- During Covid shutdowns, the transfer of checks via the mail increased the opportunity to steal check stocks for criminals to counterfeit or alter the check to fraudulent purposes.
- Banks have seen check fraud losses for the banks and their customers increase by multitudes of 2 to 3 times the expected amounts.

Spoofing Scams

- Less face-to-face interactions between customers and banks have increased the trust and reliance on texts and phone contacts. Criminals are taking advantage of this trust to gain access to accounts and transactions.
- The advanced ability to spoof phone numbers and texts to appear to come from the banks have circumvented security controls.

Card Fraud

- The increased use of cards to purchase items from the internet have limited in-person controls to prevent fraud.
- The ability of criminals to purchase skimmers and kits to access ATMs have increased the theft of card information on debit cards.

HOW DOES THE ABA ADDRESS THE CURRENT RISKS

Check Fraud

Fraud Directory – Establishing contact points bank-to-bank to ensure the claims are being handled quickly and efficiently

Fraud Tool-Kit – Creating an educational resource with guides for:

- Fraud type definitions and examples
- Claim process and timelines
- Resources for internal bank training
- Check fraud security and alternate payment guides

Universal Claim Form – Creating a resource that guides the user to the correct claim type to expedite and clarify the check fraud response.

Spoofing

Fraud Indicator Exchange – Establishing a resource to share suspicious account and activity information under 314(b) protections

Banks Never Ask That – An educational campaign to ensure awareness and steps to control this fraud risk.

Coordinating Bank Needs with Telecoms – Working with telephone service providers to determine the controls in their industry that can be leveraged to increase consumer protection for spoofing scams.

Card Fraud

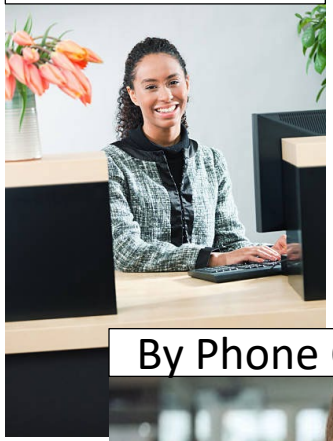
Bank Information Sharing Forums – Alignment of ABA member risk practices and initiatives in group meetings to ensure increased effectiveness across all banks.

Dedicated Policy and Regulation Resources – ABA subject matter experts monitoring and advocating regulatory and legislative actions that have the potential to mitigate card risks

FRAUD ECOSYSTEM

Banking Through Multiple Channels

At Bank Teller



At Merchant

At ATM

Online

By Phone Call

Through the Mail

Mobile Banking

HUMANS ARE THE WEAKEST LINK TO FRAUD PREVENTION

- Security And Verification of Accounts/Transactions Often Rely On A Contact With a Person
- Financial Institution Fraud Controls and Gaps
  - Account Opening: Ensuring the account owner is true and that their intent is to conduct legal banking actions.
    - Examples of Compromise Points:
      - Identity Theft
      - Business Impersonation
      - Synthetic Identity
  - Account Access: Ensuring the person accessing an account's information and ability to transact is authorized.
    - Examples of Compromise Points:
      - Cyber "hacking" attack
      - Compromised credentials (username/password)
      - Compromised security codes leading to account-takeover (ATO)
  - Account Transactions: Ensuring the transaction mirrors the intent of the account owner
    - Examples of Compromise Points:
      - Payment requests via email/text (Business Email Compromise)
      - Spoofed texts/calls
      - Stolen checks
      - Stolen credit/debit card information
      - Compromised security codes leading to an unauthorized transaction

FRAUD EVOLUTION

Fraud is a business reliant on high rewards for low exposure

- In-person to Digital:
  - Digital Banking allows a criminal the ability to mask their identity
- Days to seconds:
  - Faster transaction types limit the time a criminal is exposed in the event
- Bots and AI:
  - Cyber tools allow criminals to gather data and consolidate information a target more quickly and efficiently
- Social Media:
  - People are exposing personal data at higher rates than seen in the past decade.

Fraud Protection is reliant on consistent and controlled transactions

- Digital controls:
  - Biometrics, tokes and one-time passcodes
  - Geo location
- Faster Transactions:
  - Thresholds on accounts and customer education
  - Greater adoption of transactions to indicate true client behavior
- Media Campaigns:
  - Client familiarity and monitoring of social media offer a new resource for education
  - Social media accounts offer information to vet the true identity of the account applicant

FRAUD PREVENTION AND DETECTION OPERATIONS

Regulatory and Audit Focus

- The OCC and CFPB are focusing on fraud controls in institutions at higher levels than prior reviews.
  - Fraud programs must have governance, metrics, and true policy/procedural evidence.
  - Fraud is part of all reviews and therefore can have observations in audits/exams for BSA/AML, Payment Operations, Account Controls, Loans, Operational Risk Events, etc.
  - Customer complaints are sourced to uncover the issues that may indicate bank control gaps.
  - Failure of fraud managers, senior and executives to fully understand and be able to communicate their controls are being noted in exams.

MANAGING FRAUD RISK

- Clear 2nd Line of Defense Guidance of the Goals
- Methods of Challenging 1st Line of Defense
- Measurement and Testing

TOOLS FOR FRAUD PREVENTION AND DETECTION

Systems

Advantages

- Large data sets
- Realtime capabilities
- 24-hour capability
- Behavioral Analytics

Disadvantages

- Coordination of data and results across platforms
- Siloed technology
- Staff to monitor system rules and performance

Staff

Advantages

- Agility to move across “gray area” scenarios
- Ability to manage changes through procedures
- Live customer experience

Disadvantages

- Cost
- Skill Set
- Siloed Groups

Education

Advantages

- Standard methods to inform customers and staff
- Ensure staff has basic skills
- Positive client experience from fraud group

Disadvantages

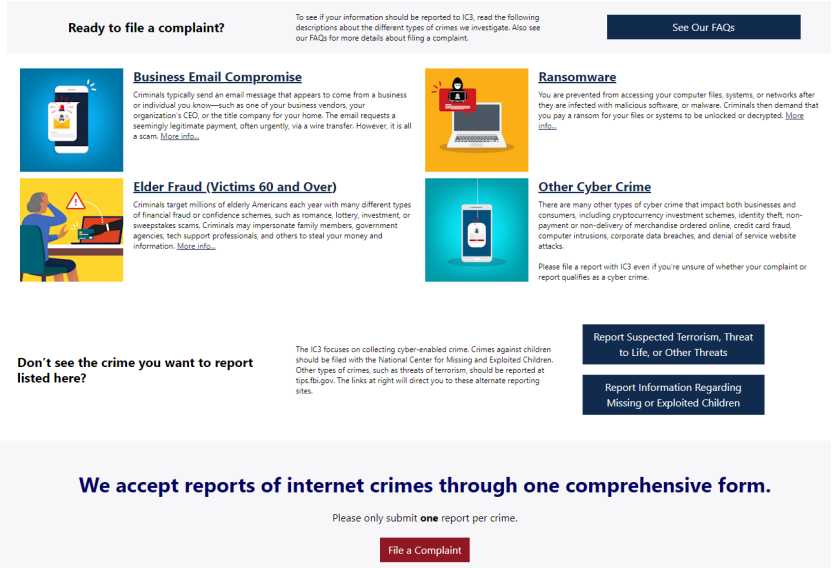
- Staffing
- Client adoption

1st Line of Defense - Fraud Investigation Themes

Who is conducting the transaction?	Were they verified?
Is the document, transfer information internally consistent?	Does everything on your screen make senses?
Is the transaction externally consistent?	When compared to the expected transactions, does this transaction appear similar or has it been pre-approved? Is this a transaction type used by your client?
Does this transaction follow your expected process?	Have there been any exceptions to the process?

Filing with the Law Enforcement

ic3.gov – Fraud Complaint Process



Madison County, MS Government
March 25 ·

Media Release

Monday, March 25, 2024

The Madison County Board of Supervisors was informed of a fraudulent financial cyber event Tuesday, March 19, 2024. The event resulted in $2,741,243.69 in funds being sent to a fraudulent vendor, who presented themselves as a current vendor.

Following the notification, the first thing the Board did was call-in law enforcement officials that include the Madison County Sheriff's office, the United States Secret Service, the Attorney General's office, the State Auditor's office, and the Federal Bureau of Investigation (FBI) to launch a national and international investigation. The investigation is in its infancy; and an update will be held once investigators have more information.

Additional safety measures have been put into place to ensure the safety of taxpayer dollars. The County Administrator will announce the new controls during the next Board of Supervisors meeting in April.

148 60 comments 33 shares

Clovis CPA Indicted for Stealing over $1 Million from a Bank

Kenneth Gould, 65, of Clovis was charged with bank larceny for stealing over $1 million from a federally insured financial institutio

According to court documents, Gould was a CPA in Clovis who owned and operated a payroll services company. From October 2 through March 2018, he initiated over 90 fraudulent Automated Clearing House (ACH) payments totaling over $20 million from on his clients' accounts to his payroll company's account at the same bank. An ACH payment is a type of Electronic Funds Transfer move money from one bank account to another account.

Based on its prior business relationship with Gould, the bank credited the fraudulent ACH payments to the payroll company's account before it realized there were insufficient funds to cover the payments, denied them, and attempted to recover its money.

Over $1 million of the credited funds, however, was gone because Gould withdrew the money while the payments were pending. Gould withdrew the money in cash, cashier's checks, and online transfers to other accounts to which he had access.
The bank made several demands to Gould for repayment. He repeatedly promised to repay the funds, but never did so.

Mississippi Man Pleads Guilty to Conspiracy to Commit Wire Fraud and Money Laundering

RYAN P. MULLEN, age 42 and a resident of Jayess, Mississippi, pleaded guilty today to one count of conspiracy to commit wire fraud and one count of conspiracy to commit money laundering

MULLEN and co-defendants used several shell Louisiana corporations, devoid of assets, to defraud a Georgia based merchant cash company. **MULLEN** created fake vendor accounts for the corporations, and **MULLEN** created falsified bank records for the companies. **MULLEN** then used an alias and represented himself to be a broker for the shell corporations he helped create.

Through the aid of another broker, **MULLEN** supplied the victim merchant cash advance company with the fake vendor accounts and false bank records in order to obtain funding. The victim cash advance company approved the advances and began to electronically wire the co-defendants millions of dollars in advances.

The funds were laundered a portion of the funds through payments and transfers. The resulting overall losses to the victim were approximately $6.4 million.

Questions?