



Building Success. Together.

Managing Cyber, Fraud and Other Operational Risk Challenges

John Carlson
VP Cybersecurity Regulation and Resilience, ABA

Maine Bankers Association
April 26, 2023

Agenda

- A bit about me
- Top cybersecurity, fraud, and other operational risks
- Cyber Regulatory Issues:
 - Cyber incident notification requirements
 - Third party risk management of the cores, cloud service providers and fintechs
- Fraud trends
- Physical security trends
- Emerging risks
- ABA efforts and resources
- USG resources

A Bit About John Carlson



- Vice president of cybersecurity regulation and resilience at the American Bankers Association
- Amazon Web Services (global financial services industry lead for security assurance),
- Financial Services Information Sharing and Analysis Center (chief of staff),
- BITS/Financial Services Roundtable (executive vice president)
- Morgan Stanley (managing director of operational risk)
- Office of the Comptroller of the Currency (director of bank technology)
- U.S. Office of Management and Budget (budget analyst)
- Federal Reserve Bank of Boston (senior analyst)
- Education: Masters of Public Policy from the Kennedy School of Government at Harvard University and a BA from the University of Maryland
- Contact: Email: jcarlson@aba.com; Tel: 202.663.5589

Top Cyber Issues: Adversaries, Motivations and Attacks

- 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

2022 Verizon Breach Report

- The biggest target in data breaches, as in previous years, is that of credentials such as usernames and passwords.
- Social engineering has increased from 22% to nearly 35% as an attack type.
 - Social engineering = use of deception to manipulate individuals into divulging confidential/personal information that is then used for fraudulent purposes.
- Business Email Compromise (BEC) for social engineering in 2021 jumped 15 times over 2020.
 - BEC = target employees (often executives) with access to company finances and trick them into making wire transfers.
- 80% of breaches identified by external parties.
- 10% of breaches involved some form of ransomware.

2022 FBI Internet Crime Compliant Center (IC3)

- The IC3 received 800,944 complaints
 - 5 percent decrease from 2021
 - However, the potential total loss has grown from \$6.9 billion in 2021 to more than \$10.2 billion in 2022
- Top victim losses (2022):
 - Investment: \$3.311 billion
 - BEC: \$2.742 billion
 - Tech Support: \$807 million
 - Personal data breach: \$742 million
 - Real Estate: \$397 million
 - Non-payment/non-delivery: \$282 million
 - Check Card/Check Fraud: \$264 million
 - Government impersonation: \$241 million
 - ID theft: \$189 million

FinCEN Financial Trend Analysis: Ransomware

- Financial Crimes Enforcement Network (FinCEN) released results of its Financial Trend Analysis of ransomware-related Bank Secrecy Act (BSA) filings for 2021 in Nov 2022.
 - Ransomware continues to threaten critical U.S. infrastructure, businesses and the public, and the threats are expanding significantly.
 - Filings substantially increased from 487 in 2020 to 1,489 in 2021, and the value of ransomware-related BSA filings in 2021 approached \$1.2 billion—a 188% increase compared to the previous year.
 - A substantial number of ransomware attacks appear to be connected to actors in Russia with roughly 75% of the ransomware-related incidents reported to FinCEN during the second half of 2021 pertained to Russia-related ransomware variants.

Cyber is a Top Risk of Community Banks

- Based on January 2023 ABA Banking and Risk Compliance Outlook Survey, 74% of 250 community bankers listed cyber/IT security risk in their top three priorities over the next 18 months.
- Based on Risk Management Association (RMA) 10th Annual Community Bank Survey, 85% of the community bank executives surveyed cited cybersecurity risk as one of the top six priorities.

Increasing Cyber Regulatory Requirements

- Federal:
 - Computer Security Incident Notification Rule (FDIC/FRB/OCC)
 - Proposed Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure, proposed amendments to Reg S-P, Reg SCI and Exchange Act (SEC)
 - Cyber Incident Reporting for Critical Infrastructure Act of 2022 (DHS/CISA proposal forthcoming)
 - FFIEC Information Technology Booklets (e.g., Information Security, Outsourcing Technology Services, Architecture, Infrastructure and Operations, Business Continuity Management)
 - FFIEC Cybersecurity Assessment Tool (CAT)
 - GLBA Safeguards Rule
- State:
 - Too many to enumerate but one that many are focusing on is the New York State Department of Financial Services (“NYDFS”) proposed amendments to Cybersecurity Requirements for Financial Services Companies

Example: Cyber Incident Reporting Requirements

24-hour reporting of ransomware payment to the Cybersecurity and Infrastructure Security Agency (CISA)*

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

36-hour incident notification to primary regulator (FRB,OCC,FDIC)

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

72-hour reporting to CISA *

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

4 business days SEC disclosure*

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.

*awaiting final rule

Increasing Focus on 3rd Party Risk Management: Cloud

- US Treasury Report
 - 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.

Increasing Focus on 3rd Party Risk Management: Cloud

- US Treasury 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.
 - Proposes an action plan :
 - Establishing a “Cloud Services Steering Group” with participation of federal financial regulators to promote closer domestic cooperation among U.S. regulators;
 - Facilitating further engagement between the financial sector and CSP
 - Conducting tabletop exercises with industry;
 - Reviewing sector-wide incident protocols in light of growing reliance on cloud services;
 - Considering ways to appropriately measure cloud service dependencies across the sector and assessing systemic concentration and related risks on a sector-wide basis;
 - Identifying ways to foster effective risk management practices in the financial services industry;\
 - Continuing 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
 - Exploring ways to increase international collaboration and coordination on financial regulatory issues arising from cloud services.

Increasing Focus on Third Party Risk Management

- What's next?:
 - FDIC, FRB, OCC updated guidance on managing risks associated with third-party relationships (in response to July 2021 notice)
 - Financial Stability Board consultation on third-party risk management and oversight for critical providers

Cyber Risk Insurance Issues

- Increasing premiums
- Limits on coverage
- Concerns with proposals by to exempt big “state-backed” cyber attacks from standard insurance policies
- Biden National Strategy includes a brief reference to exploring a Federal cyber insurance backdrop which contemplates the government’s liability and response to a too-big-to-fail scenario or catastrophic cyber incident.

Fraud

- Top fraud risks:
 - Check
 - Imposter Fraud
 - Elder exploitation
 - Business email compromise
 - Peer to Peer Payments (P2P)
- Fraud against US and State Covid Assistance
- Government actions:
 - Increased enforcement for Crypto
 - Compliance with AML/BSA for DeFi

Top Fraud Risks


- Check Fraud
 - The oldest type of fraud in America has become the newest threat to banks.
 - The volume at which checks are being stolen from the U.S. mail system, the organization of criminal groups, and the convergence of street-level tactics with open access to social media and the dark market have flooded the multiple deposit points (remote, ATM & branch) at banks.
 - Three types of check fraud:
 - Forged endorsements – normally stolen check by less sophisticated criminal
 - Counterfeit – increased level of skill, with availability of check stock, computer programs, account information on dark market adds to prevalence of problem
 - Altered/"Washed" – most common fraudulently deposited checks. Attributing factor is the increased focus by organized criminal groups stealing U.S. mail.

What's Happening on the Street



Theft of Arrow Key



**UNITED STATES POSTAL
INSPECTION SERVICE**

ABOUTCAREERSTIPS & PREVENTIONNEWSREPORT

Scam Article

Check Washing

Last updated 05/01/2019National

Have you ever sent a check that was cashed, but the recipient said it never arrived? You may be the victim of check washing. Check washing scams involve changing the payee names and often the dollar amounts on checks and fraudulently depositing them. Occasionally, these checks are stolen from mailboxes and washed in chemicals to remove the ink. Some scammers will even use copiers or scanners to print fake copies of a check. In fact, Postal Inspectors recover more than \$1 billion in counterfeit checks and money orders every year, but you can take steps to protect yourself.

Check Washing (Identity Theft)

A gang of scammers started an illegal check washing scam to bankroll their drug habit. Watch to learn more about check washing.



Check Washing (Identity Theft)

Watch laterShare

Top Fraud Risks

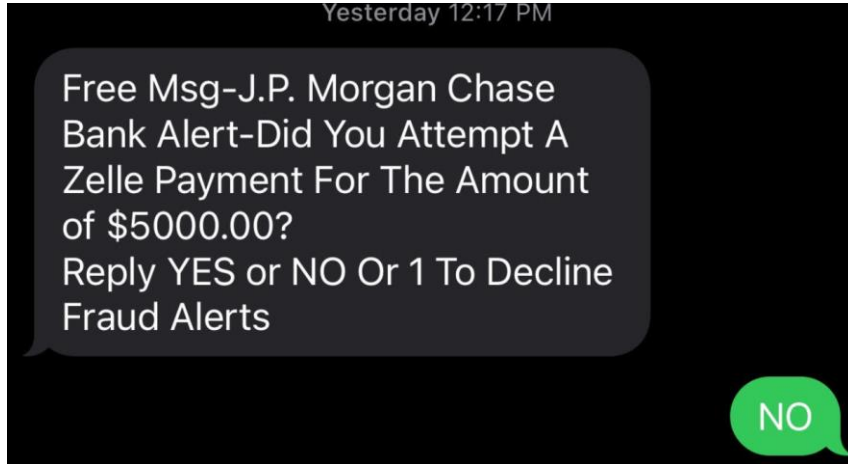
- Imposter Fraud

- External frauds like this have many subtypes; to name a few: Romance, Exploitation, Investment and even Puppy scams.
- Opportunity is created when the fraudster makes a “personal” connection with a victim and introduces a sense of urgency to speed up the victim’s decision-making process on sending money based on promises never intended to be met.
- Fraudsters deploy phishing (via email), smishing (via SMS), and vishing (via telephone) tactics to social engineer personal information used to manipulate the victim into sending money from, to, or through their bank account(s).
- Fraudster remains anonymous during the bank account money movement, using account takeover tactics or witting/unwitting customers to mule the money back to the fraudster.

Top Fraud Risks

- Elder Exploitation
 - Elders are commonly known to have a lifetime savings or regular flow of automated income like social security benefits, 401(k) distributions or annuity payments.
 - This makes them prime targets for organized fraud groups.
 - Similar imposter fraud tactics are used to exploit vulnerabilities like being a widow(er) (romance scams) or becoming familiar with new technologies in this online era (technology help scams), to name a few.
- Business Email Compromise/Email Account Compromise (BEC/EAC)
 - Social engineering along with electronic messaging creates an opportunity for the fraudster to implement anonymity (or pseudonymity) and speed up financial decisions by customers (businesses and consumers), making this the most prolific cyber-enabled fraud.
 - Fraudsters easily introduce a sense of urgency into the equation. and decisions are made to move significant amounts of money from the victim's bank account to a bank account controlled by the fraudster.
 - Once the customer makes what appears to be an authorized payment and the beneficiary account is confirmed, the money transfer can only be detected and attempted to be stopped as fraudulent if the victim contacts the bank quickly upon discovery.

P2P Fraud



- After victim responds (yes or no), fraudster calls them
- Fraudster socializes username and initiates password change
 - To defeat 2 step auth, fraudster keeps victim on phone and gets passcode to change password
- Password is changed and P2P payments are made to fraudsters accounts

Crypto & DeFi

- US Securities and Exchange (SEC) and Commodity Futures Trading Commission (CFTC) have stepped up enforcement of crypto exchanges and DeFi
 - Enforcement actions against Binance, Coinbase, FTX, Gemini, Kracken
 - SEC's Office of Investor Education and Advocacy caution: "Investments in crypto asset securities can be exceptionally volatile and speculative, and the platforms where investors buy, sell, borrow, or lend these securities may lack important protections for investors. The risk of loss for individual investors who participate in transactions involving crypto assets, including crypto asset securities, remains significant."
- Treasury Report Recommends More BSA Enforcement for 'DeFi' Sector
 - Many existing decentralized finance services covered by the Bank Secrecy Act fail to comply with anti-money laundering and counterterrorism financing obligations, which illicit actors exploit
 - A host of illicit actors—from ransomware criminals to North Korea—rely on DeFi services to transfer and launder funds

Physical Security Incidents

- Natural
 - Weather-related (hurricanes, tornadoes, etc.)
 - Earthquakes
 - Wildfires
- Man-made
 - Branch Robberies
 - ATM Crimes
 - Workplace Violence
 - Domestic Violence, Disgruntled Employees, Disgruntled Customers, Active Aggressors/Shooters
 - Violent Extremists
 - Civil Unrest

Physical Threat Actors: Motivations

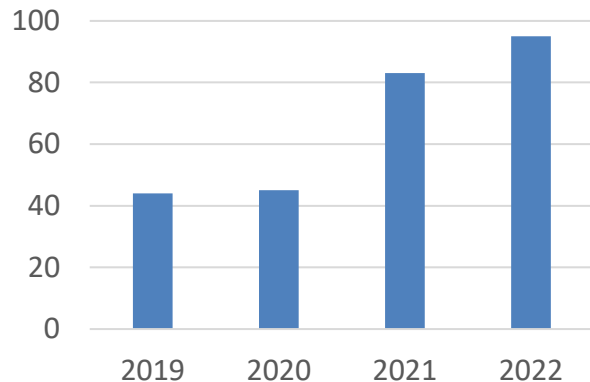
- Violent Extremists
 - Violent, criminal attacks against soft targets
 - Inspired by a mix of ideological, sociopolitical, and personal grievances
 - Domestic Violent Extremists (DVEs). Ideological goals stemming from domestic influences, such as racial bias and anti-government sentiment
 - Homegrown Violent Extremists (HVEs). Radicalized primarily in the U.S. and inspired by, but not receiving individualized direction from, foreign terrorist organizations

ATM Crimes: Cyber/Data Attacks

- Skimming: Installation of device to capture data from card mag strips
- Shimming: Interception/manipulation of information between EMV card and the chip interface of the card reader
- Eavesdropping: Installation of device onto the internal motorized card reader to intercept transferred data from customers' cards.
- Transaction Reversal Fraud: Manipulation of ATM cash withdrawals to appear that cash not dispensed; reversal message generated.
- Black Box: Connection of device that sends dispense commands directly to the ATM cash dispenser in order to "Cash-Out" the ATM.
- Cash Out or Jackpotting: Installation of malware that sends dispense commands directly to the ATM cash dispenser.

ATM Crimes: Physical Attacks

- ATM Burglaries
 - Hook and Chain
 - Brute Force
 - Ram Raid
- Robberies of ATM Servicers and Technicians



ABA Efforts to Address Cyber Risks (1/3)

- Engagement w/ USG on National Cybersecurity Strategy
 - Released in early March
 - Key Proposals:
 - Shift liability for software products and services to promote secure development practices,
 - Harmonize/converge regulations to reduce the burden of compliance,
 - 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,
 - Exploring a Federal cyber insurance backdrop.
 - Key engagement points: US Congress, White House, US Treasury Department, Department of Homeland Security's Cybersecurity, and Infrastructure Agency (CISA), National Institutes of Standards and Technology (NIST)

ABA Efforts to Address Cyber Risks (2/3)

- Treasury Cloud Report
 - ABA leadership in the Financial Services Sector Coordinating Council
 - Focus on enhancing transparency, assessing concentration risk and dependencies
 - Engage core service providers through the ABA Core Platforms Committee
 - Encourage use of the free Cyber Risk Institute Profile (which is aligned with the Cloud Security Alliance's Cloud Capability Matrix) to reduce the time required to demonstrate compliance with regulatory requirements and cyber standards.

ABA Efforts to Address Cyber Risks (1/3)

- Post quantum computing risk mitigation for encryption
- Support for .bank
- Sheltered Harbor
- 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>
- “Hamilton” series cyber exercises (with US Treasury)
- ABA Risk Management School and Courses on Cyber, Business Continuity, and Third Party Risk

ABA Efforts to Address Fraud Risks

- ABA 314b Fraud Information Exchange (AfieX)
 - Intelligence sharing network to enhance banks' ability to identify and defend against fraudulent transactions
 - Aggregates & centralizes suspect account information associated with potential bad actors and/or fraudulent accounts, allowing participants to proactively identify and act against future transactions
 - Aligns to FinCEN's expectation that financial institutions share data to identify and report on activities associated with fraud, money laundering and terrorist financing

FinCEN's expectation that financial institutions share data to identify and report on activities associated with fraud, leading to money laundering and terrorist financing

[See FinCEN's Section 314\(b\) Fact Sheet](#) (Dec. 2020)

 An official website of the United States Government



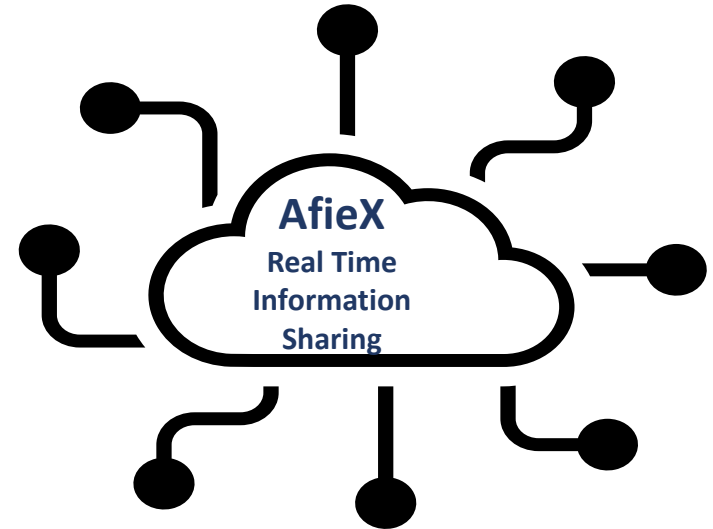
FinCEN Director Emphasizes Importance of Information Sharing Among Financial Institutions

Contact: Office of Strategic Communications, 703-905-3770
Immediate Release: December 10, 2020

WASHINGTON—Financial Crimes Enforcement Network (FinCEN) Director Kenneth A. Blanco today discussed how information sharing is critical to identifying, reporting, and preventing financial crime. In his [remarks](#) to the annual American Bankers Association/American Bar Association Financial Crimes Enforcement Conference, Director Blanco provided important clarification on FinCEN's information sharing program under [Section 314\(b\)](#) of the USA PATRIOT Act, and announced that FinCEN is issuing a new [314\(b\) Fact Sheet](#) and [rescinding](#) previously issued guidance (FIN-2009-G002) as well as a former administrative ruling (FIN-2012-R006) (parts of which are incorporated into the guidance in the new 314(b) Fact Sheet).

Section 314(b) of the USA PATRIOT Act is an important tool for combatting financial crime. It provides financial institutions with the ability to share information with one another, under a safe harbor provision that offers protections from civil liability, in order to better identify and report potential money laundering or terrorist financing. After carefully considering feedback from the financial industry, FinCEN is providing three main clarifications:

- A financial institution may share information relating to activities that it suspects may involve possible terrorist financing or money laundering. Although this may include circumstances in which a financial institution has information about activities it suspects involve the proceeds of a specified unlawful activity (SUA), financial institutions do *not* need to have specific



AfieX is an Interoperable Application that Enhances Information Exchange Using Standardized Data & Communications

This is a “plug-in” utility external to the banks IT infrastructure

- Access via secure API that feeds into banks
- Delivery options are API automation or user interface

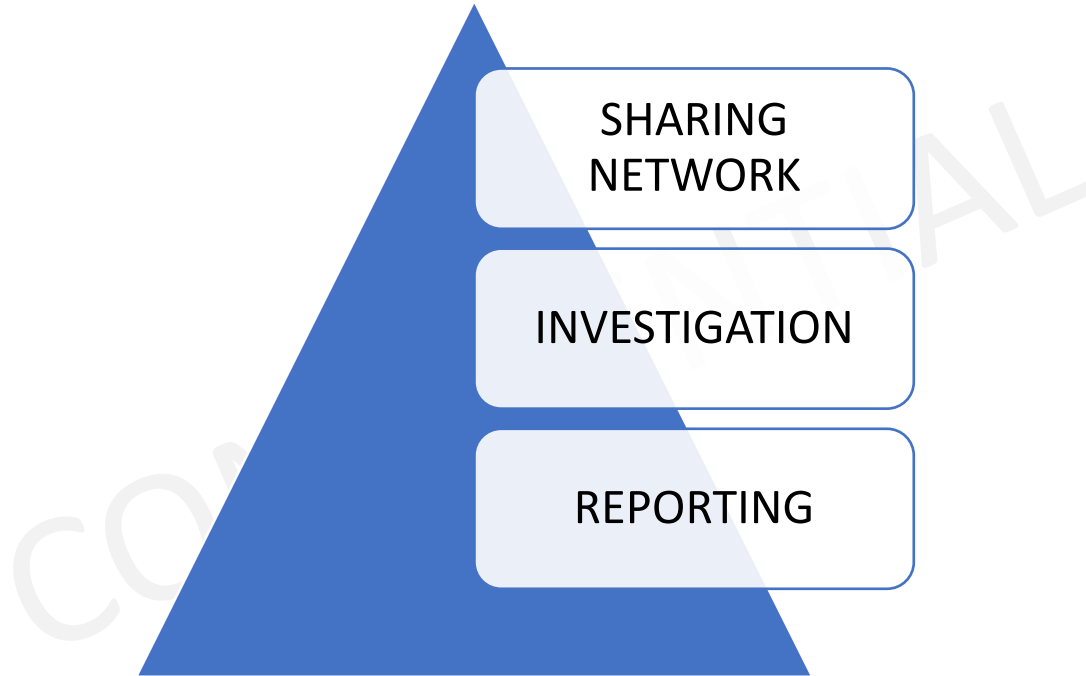
No specific media or type of communication is currently being used to exchange information between banks under 314b

- Phone, email, and other means

Sharing will be real-time for consortium members

- Data available to all for fraud prevention, cyber crime & SAR reporting
- Secure, easy queries of derogatory source data
- Unified data aggregation from disparate bank systems/platforms

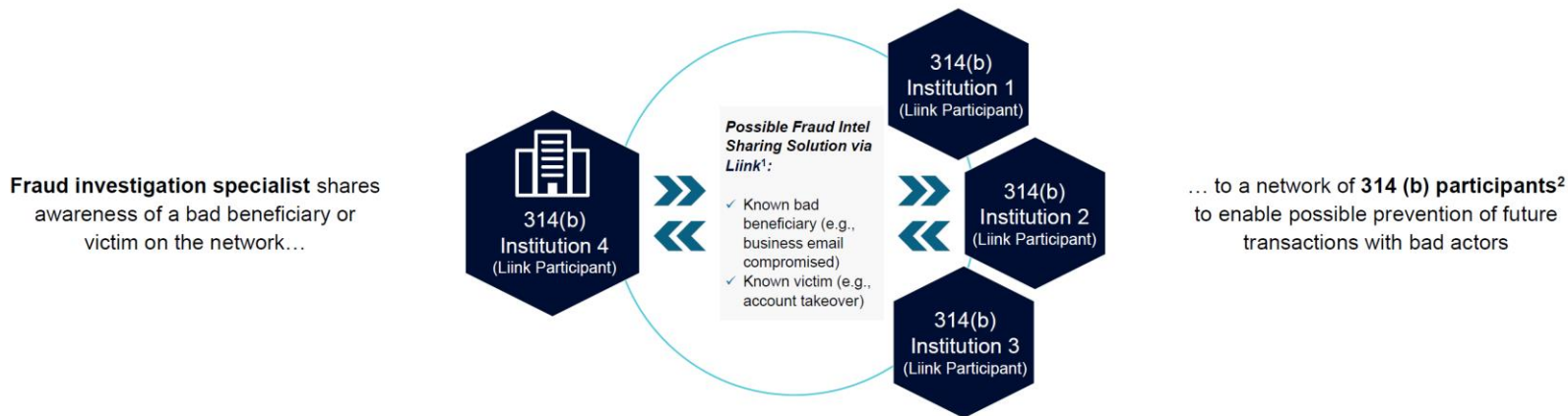
Clean, timely data equals account holder validation and produces Quality SARs to Law Enforcement to deter future bad conduct by the actor



Fraud Intel Sharing under 314(b)

Industry problem statement: Reducing instances of fraud relies on intelligent logic and robust data sets, but accessing relevant data is time-intensive, complex, and requires exchanging information securely.

A possible solution¹: Supplementing the fraud monitoring process with new data and insights could reduce both false positives and fraud cases



Efficient



Structured



Fast



Secure



Scalable

Consumer Education: #BanksNeverAskThat Campaign

Use humorous videos, social posts, digital signage and more to highlight questions banks would never ask their customers.

Free for ABA Members:

<https://www.banksneveraskthat.com/>



Emerging Risks

- Post quantum computing impact on widely used public key encryption
- Artificial intelligence/Chat GPT impact on phishing, fraud, mis/dis-information, cyber attacks

ABA Resources for Cyber Security

- 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

ABA Resources for Physical Security

- **ATM Security**

- ABA Advisory: ATM Service Technician Robberies
- ATM Risk Assessment
- ATM Security Statutes

- **Bank Robberies**

- ABA Toolbox on Bank Robbery Deterrence
- ABA Bank Capture System
- Customizable Guides: Robbery Training; Branch Opening
- Robbery and Bank Security (Online Training)

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>

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

John Carlson, Vice President for Cybersecurity Regulation and Resilience
Jcarlson@aba.com