



# Bank Operations and Cybersecurity



Mr. Stephen Kenneally, Mr. Jim  
Hitchcock, and Mr. John Carlson  
American Bankers Association

## Trend Talk: The Evolution of Payments in 2023

## Roadmap

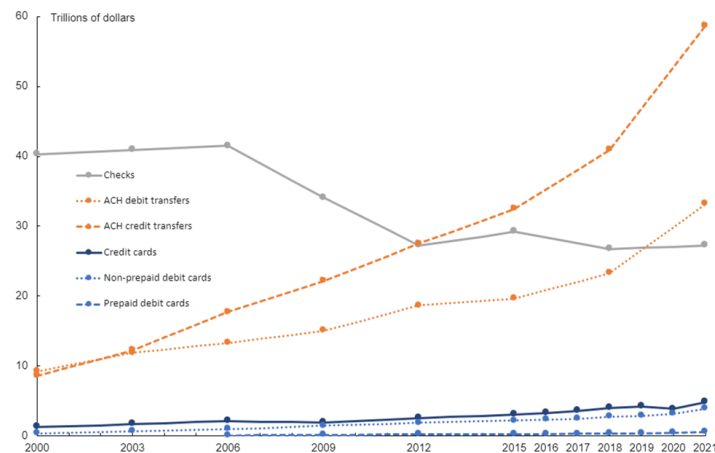
- Federal Reserve Payments Study
- TCH Real Time Payments Are Live
- FedNow Launched July 20, 2023
- Zelle
- Coin Circulation
- Digital Asset Framework
  - Cryptocurrency
  - CBDC
  - Stablecoin
  - Tokenized Deposits
  - NFTs

## 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 Chair, Faster Payments Alliance Board Member

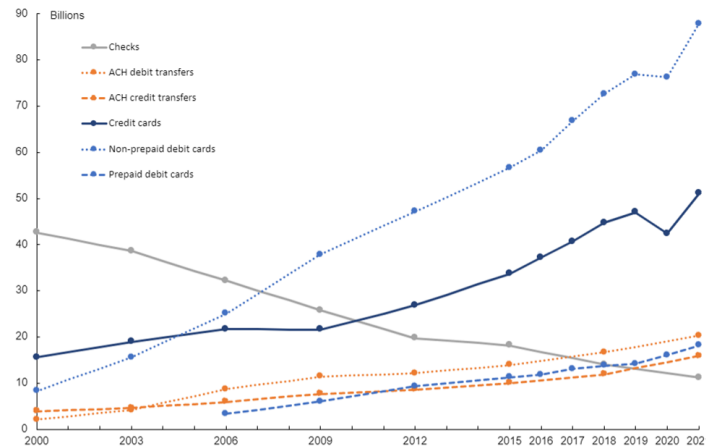
## Trends in non-cash payments by dollar value 2000-2021

Federal Reserve Survey



## Trends in non-cash payments by transaction 2000-2021

Federal Reserve Survey



aba.com | 1-800-BANKERS

5



## The Clearing House Real Time Payments Network

### Overview

- Launched in November 2017 and currently implemented by The Clearing House (TCH) with 300+ banks live
- Allows US banks to offer 24/7/365 real-time payment services capped at \$1 million per transaction
- Currently reaches over half 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

- Will compete 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

aba.com | 1-800-BANKERS

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

6



# FedNow

## Overview

- Currently being developed by the Federal Reserve
- Will allow banks in the US to offer 24/7/365 real-time payment services
- Launching July 2023 (launched 7/20/23)

## Process

- Will enable all banks to provide real-time payments through their master accounts held at the Federal Reserve
- Will ease delays and built-up financial obligations between banks that could present risks to the financial system
- Will initially support 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

## 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
Vizio 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.

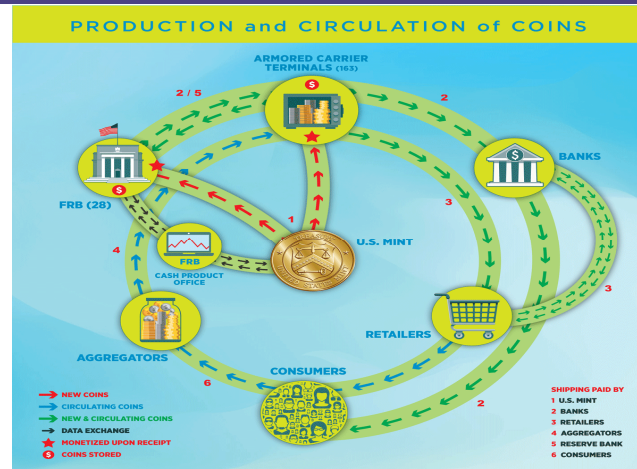
### Key Issues

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

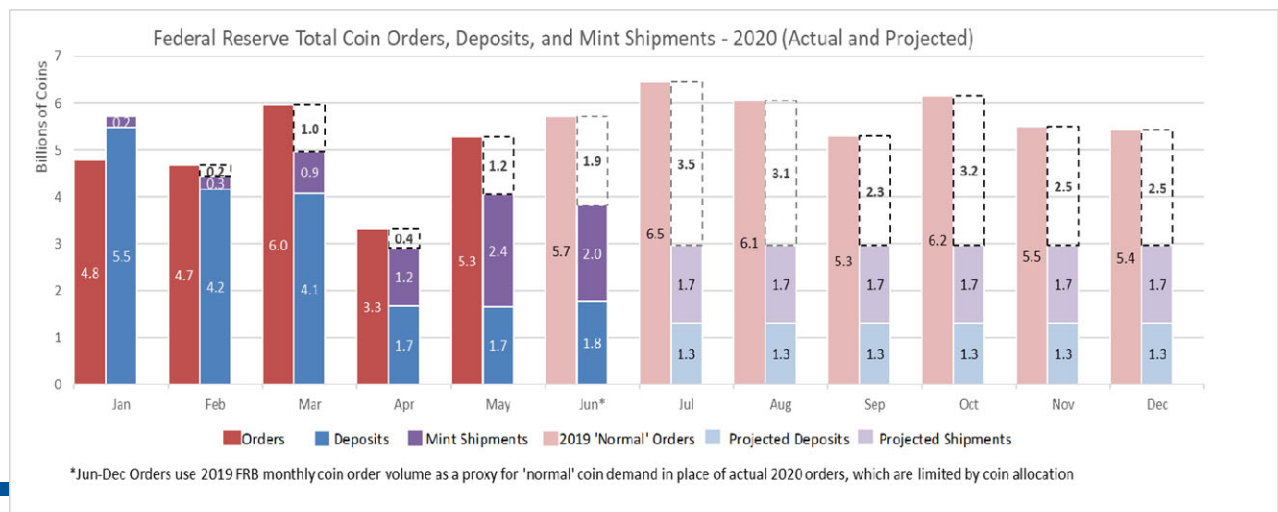
## FedNow/TCH RTP/Zelle

	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 <u>will be</u> processed and master account will go into overdraft	Payment <u>will not be</u> processed	Payment <u>will not be</u> 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.

# Circulation of Coin in Normal Times



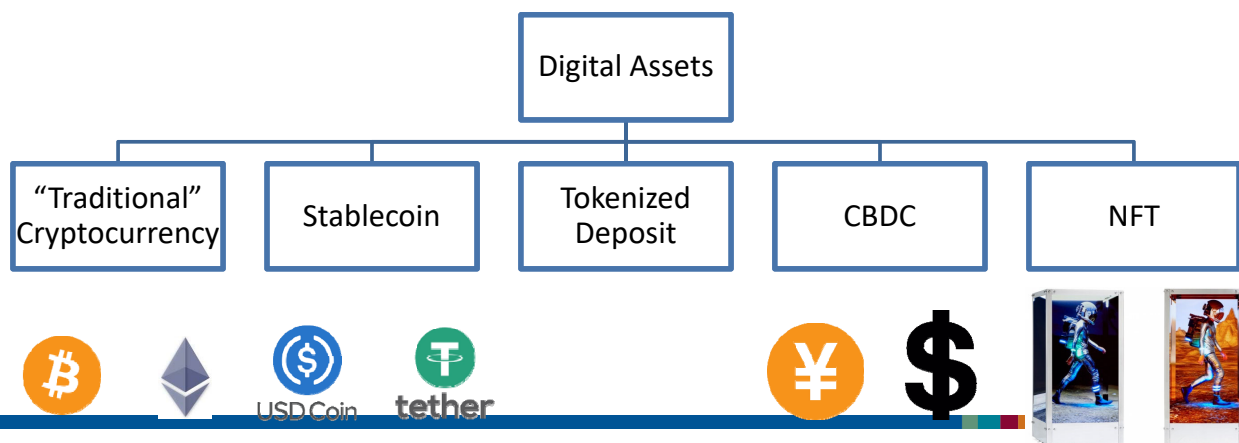
# US Coin Supply and Demand



## Coin Circulation Tools

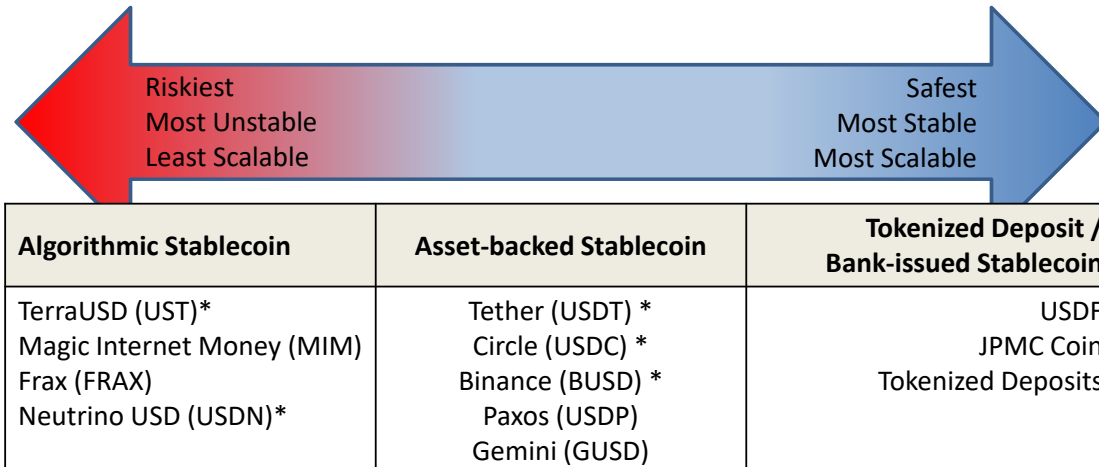
- Encourage consumers to use exact change
- Encourage consumers to “cash out” coins at banks and coin aggregators.
  - Coin drives for employees.
  - Rewards for customers.
- Round up/round down deposits (Banks).
- Round up/round down purchases (Merchants).

## Digital Asset Framework





## Not all stablecoins are the same



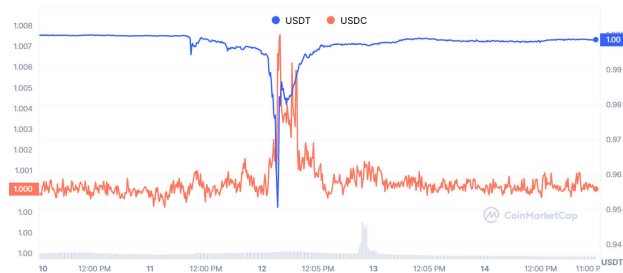
aba.com | 1-800-BANKERS  
\*De-pegged

15



## How stable?

Tether and USDC – May 2022



Tether and USDC – March 2023

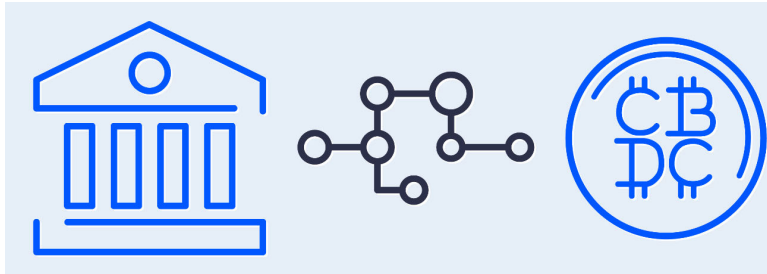


aba.com | 1-800-BANKERS

16



## Central Bank Digital Currencies (CBDC)



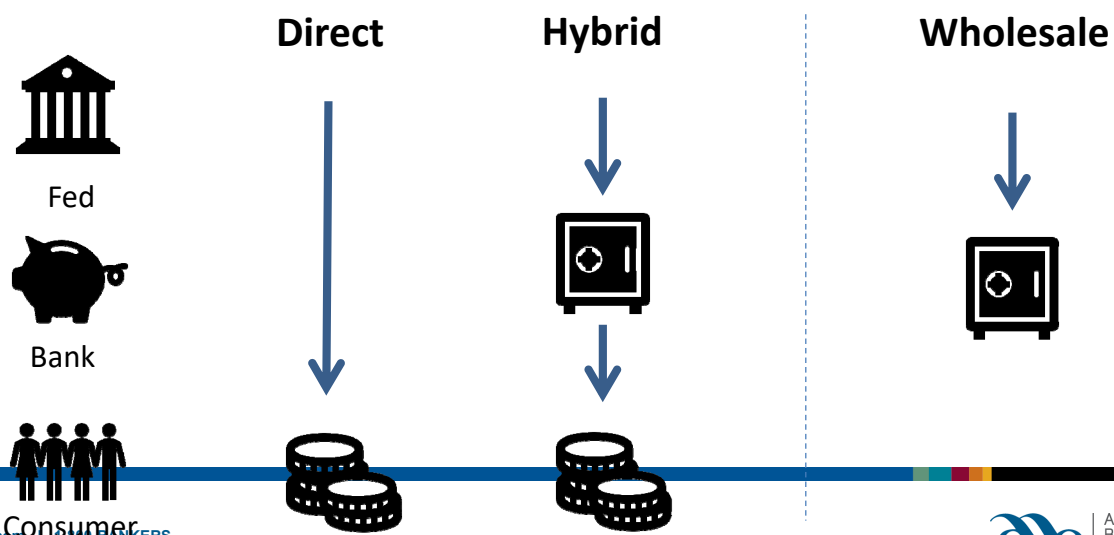
- Digital token issued by and held as a liability of the Federal Reserve
- Fundamental change in a consumer's relationship with the Fed

aba.com | 1-800-BANKERS

17



## CBDC Models



aba.com | 1-800-BANKERS

18



## No compelling case for CBDC in U.S.

### Opportunity

- Financial Inclusion
- International Competitiveness
- Cross Border

### Risks

- Deposit Substitution
- Financial Stability
- Big Tech's Role
- Fed Balance Sheet
- Privacy
- Enforcement of AML/KYC/Sanctions

## American Bankers Association

Steve Kenneally  
Senior Vice President, Payments  
American Bankers Association  
[skenneally@aba.com](mailto:skenneally@aba.com)  
202-663-5147

# The State of Fraud

Jim Hitchcock, ABA  
Maryland Bankers Association  
Maryland Banking School  
August 3, 2023

aba.com1-800-BANKERS

21



## Agenda

- What's Old is New Again
  - Check Fraud on the rise as we move deeper into 2023
  - Progress made by industry, Postal Service and ABA
- The next Check Fraud
  - Mules via Synthetics
  - AI (BOTs, Deepfakes, & ChatGPT)
- Appendix / Resources
  - ABA Tools
  - Advocacy in motion
  - Law Enforcement Assistance Available to Track Money

aba.com1-800-BANKERS

22



## Check Fraud Continues



Mail Theft



Dark Net Markets vs Public Channels



Misconceptions with Banks

Fraud Tech

Positive Pay

Reg CC holds and Returns

[aba.com](http://aba.com) 1-800-BANKERS

23



## What's Happening on the Street



Theft of Arrow Key



UNITED STATES POSTAL INSPECTION SERVICE

ABOUT CAREERS TIPS & PREVENTION NEWS REPORT

### Check Washing

Team Article

Last updated 05/01/2019 National

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 bankrupt their drug habit. Watch to learn more about check washing.

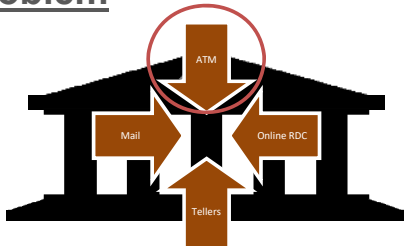
[aba.com](http://aba.com) 1-800-BANKERS

24



## Take Eye off the Basics – Check Fraud

### Problem



### FinCEN SAR Statistics

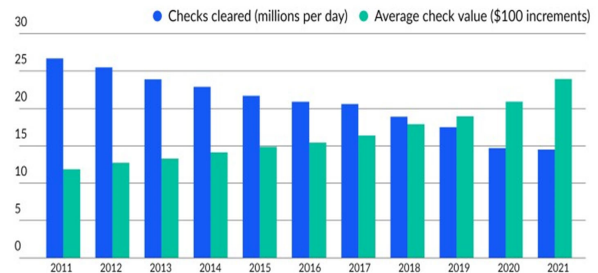
Suspicious Activity Category	Suspicious Activity Type	2014	2021	2022
Fraud	ACH	24,904	176,911	
	Check	96,786	350,000	680,000
	Credit/Debit card	75,496	140,327	

aba.com1-800-BANKERS

25

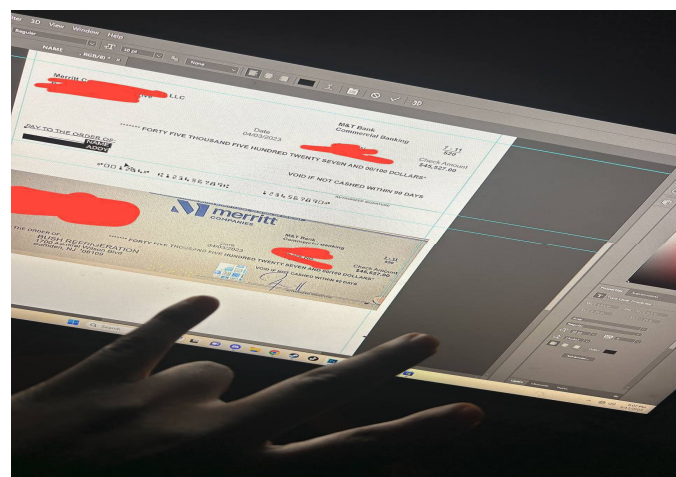
### Challenges

- Created backlogs in check warranty claims
- Availability of funds (Rec CC & Check 21)
- Average check value doubled last decade



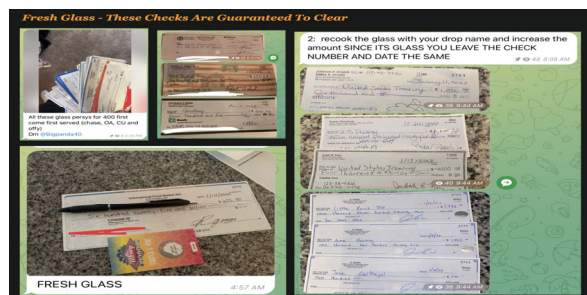
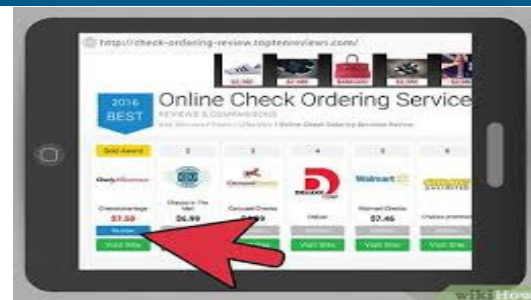
Source: Federal Reserve

## Graphic Designing Lessons – Cooking Checks



aba.com1-800-BANKERS

26



## Synthetic Businesses

**American Express LLC** Action ▼ A

6 Business Advantage Checking ▼

Account Identification: American Express LLC  
 American Express LLC Business Advantage Checking  
 Bronx NY 10455 Show More

Summary	Ledger balance:	0.00	Today's activity:	0.00
Account Detail	Current balance:	0.00	Total Holds:	0.00
Bankruptcy Case	Account available:	0.00	Float:	0.00
Account Detail	Total accessible:	0.00	Unused PRA:	0.00
Balances and Activity	Closing balance:	0.00	Related available balance:	0.00
Analysis and Statement	Last statement:	08/31/2022		
Detail				
Overdraft/UAF Detail				
Transaction History				
Expanded Transaction History				
Rate History				
Stop Plays				
Holds				
Relationships				
Float Detail				
Miscellaneous Service Charges				
Rolling 12-Month Information				
Nonmonetary History				
Flexible Groups Current Cycle				
Name and Address Remarks				

11 / All transaction Search Details

Date	Debit	Credit	Other Description	Balance
08/31/2022			Daily balance	0.00
08/31/2022	65.00		828 - Debit Memo	
08/26/2022		65.00	Daily balance	65.00
08/26/2022	10.00		799 - Service Charge	65.00
08/26/2022	143,474.47		159 - Rtn Dep Item Debit	75.00
08/26/2022		143,474.47	629 - Credit Memo	143,549.47
08/24/2022		75.00	Daily balance	143,549.47
08/24/2022	143,474.47		828 - Debit Memo	75.00
08/23/2022		143,474.47	Daily balance	143,549.47
08/23/2022		143,474.47	600 - Deposit	143,549.47
08/23/2022		143,474.47	586 - Available Float	75.00
08/23/2022		143,474.47	580 - Collectable Float	75.00
08/23/2022		143,474.00	588 - Avl Float Minus Adj	75.00
08/19/2022		75.00	Daily balance	75.00
08/19/2022	25.00		984 - Misc Service Charge	75.00
08/19/2022		100.00	600 - Deposit	100.00

aba.com1-800-BANKERS

27



## Synthetic Businesses

**NEW YORK STATE** Q Search

Services News Government COVID-19

**Entity Details**

ENTITY NAME: AMERICAN EXPRESS LLC DOS ID: 6537587

FOREIGN LEGAL NAME: FICTITIOUS NAME:

ENTITY TYPE: DOMESTIC LIMITED LIABILITY COMPANY DURATION DATE/LATEST DATE OF DISSOLUTION:

SECTION OF LAW: LIMITED LIABILITY COMPANY LAW - 203 LIMITED LIABILITY COMPANY LAW - LIMITED LIABILITY COMPANY LAW ENTITY STATUS: ACTIVE

DATE OF INITIAL DOS FILING: 07/15/2022 REASON FOR STATUS:

EFFECTIVE DATE INITIAL FILING: 07/15/2022 INACTIVE DATE:

FOREIGN FORMATION DATE: STATEMENT STATUS: CURRENT

COUNTY: BRONX NEXT STATEMENT DUE DATE: 07/31/2024

JURISDICTION: NEW YORK, UNITED STATES NFP CATEGORY:

**NAME** ENTITY DISPLAY NAME HISTORY FILING HISTORY MERGER HISTORY ASSUMED NAME HISTORY

AME

Service of Process on the Secretary of State as Agent

The Post Office address to which the Secretary of State shall mail a copy of any process against the corporation served upon the Secretary of State by personal delivery:

Name:

Address: 536 E 148TH STREET, BRONX, NY, UNITED STATES, 10455

Electronic Service of Process on the Secretary of State as agent: Not Permitted

Chief Executive Officer's Name and Address

Name:

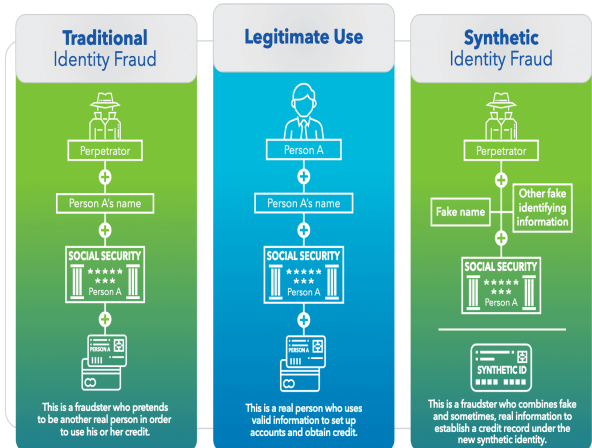
aba.com1-800-BANKERS

28



## Synthetic People (aka Mules)

- Unlike traditional identity thieves who prey on physical victims, **SIF** starts with a single piece of legitimate personal data
  - Usually, a Social Security number
  - Then builds a fake identity around it using a bogus address, phone number, and other basic information.
- Synthetics have been treated as victimless frauds and are difficult to detect, as a result also underreported for years.
- Both frauds exploit the credit bureau & credit card industry's card issuing model

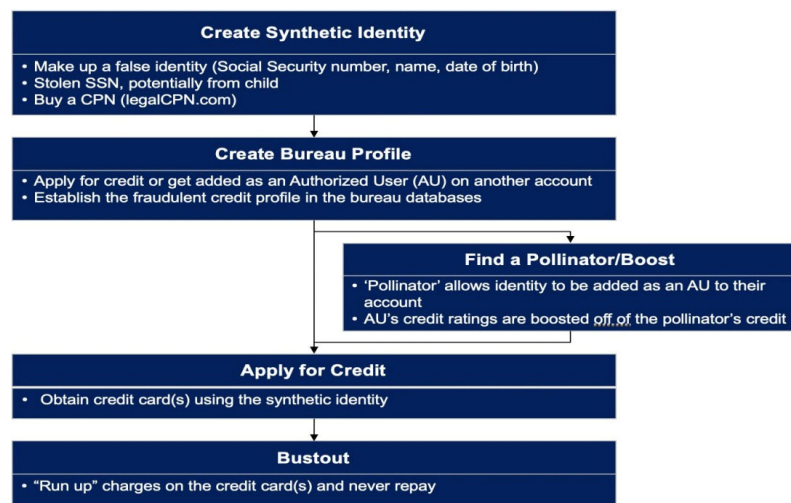


aba.com1-800-BANKERS

29



## Baking an Identity from Scratch



aba.com1-800-BANKERS

30





## Legitimate Checks but Fraudulent Funds (COVID Fraud 2.0)



12 000  
BAG NOS  
74 TEA

Oct. 21, 2022, 4:45 AM

### IRS Warns Taxpayers on False Employee Retention Credit Claims

**COLUMN**

 **Kelly Phillips Erb**  
Editor



Nosa Nobore (Giovanni)

The Employee Retention Credit was intended to encourage businesses to keep employees on their payrolls. But as the economy tightens, the IRS is warning about fraudulent schemes. Here's what you need to know.

**What would you do if I told you I could guarantee your small business a refundable tax credit of \$26,000 per employee—without ever having seen your books?**

I hope you'd run in the opposite direction.

But increasingly, employers are sticking around to hear more, and some have been convinced to claim the Employee Retention Credit, or ERC, when they might not qualify. This week, the IRS [warned businesses](#) to be cautious when third parties promise tax savings that are too good to be true.

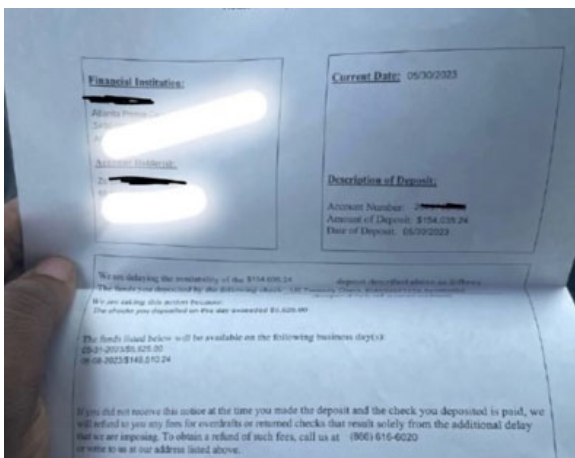
**Law Firms**

[Clark Hill](#)

**Topics**

[Amended Tax Returns](#)  
[Small Business Credits](#)  
[Payroll Tax](#)  
[Jobs Credits](#)  
[Tax Fraud](#)  
[Filing Tax Returns](#)  
[Small Businesses](#)

## Continuous Challenges for “Fraud Tech”



- Businesses are passing Authentication Tech, as they are appropriately registered
- Fraud is bypassing Reg CC Hold Notices and RDI process not counterfeit or NSF
- Altered/Legitimate Items still Pass
  - Need Collection Notice
- Positive Pay does not detect stolen checks
  - Payee Positive pay a must

# Smart Practices

## KYC & KYC

### FraudWit Quick Guide To Check Exposure Components

**Mail theft leading to check fraud has risen significantly in the past few years. A check has all the components that criminals need to stage an attack. This negatively affects both consumers and businesses as well as the financial institutions that support them.**

**Understanding the exposure risks of individual check components can help people realize what they are sending when dropping a check in the mail.**

**Payee Line:** Forged endorsement risk, especially on high dollar business checks paying other businesses.

**Example:** Check made payable to Riblets-Are-Us is stolen by fraudster, who makes fake business called Riblets-Are-Us LLC and deposits the check. Water believes check has paid legitimate payee until notified, resulting in a forged endorsement claim.

**Memo Line:** Used in counterfeiting to convince scam participants (and sometimes others) of legitimacy / validity.

**Check Sticks:** Provides layout (border and check component positions) that can be replicated when counterfeiting.

**Maker Information:** Applied to counterfeiting checks and account takeover attempts. Used to identify victim, extending to address and phone. Phone can also be used for various scams (specifically authority scams when paired with bank name).

**Bank Name:** Provides criminal with reference to bank, which can lead to account takeover attempts or authority scams.

**Check Number:** Gives check range to use when counterfeiting and provides indication on maker usage.

**Routing and Account Number:** The basic two components needed to attack a victim. These two items are often used to counterfeit checks and/or to help perpetrate certain types of ACH fraud.

**Maker Signature:** Provides victim signature to try to replicate when counterfeiting. In check washing, washed signature leaves indentation that can be traced.

**Disclaimer:** FraudWit Banks not a real bank—and never will be.

**FraudWit.com**

### Inclearing Check Fraud: Use other data beyond the check image

- BOFD
- ACH data/trial credits/claims
- Online / Deep Market Intel

### Deposit Check Fraud : Behavioral analysis

- Transactions before and after deposits
- OCR\* for both sides

### Consumers: Check your accounts

- Confirm your payments as they clear

\*Optical Character Recognition

aba.com1-800-BANKERS

33



## Which one's real? Altered or Counterfeit?

**Maryland State Retirement and Pension System**  
120 East Baltimore Street | Baltimore Maryland 21202-6700  
www.SRA.MARYLAND.GOV

Account Of: **CIERRA N**  
ID No: 41221-39

Payee No: 4122-89

Check No: 00654876

Date of Check: 12/12/2022

**PAY FIVE THOUSAND SIX HUNDRED THIRTY AND 00/100 DOLLARS**

To the **CIERRA N**  
order  
of

**M&T Bank**  
Manufacturers and Traders Trust Company  
Commercial Banking

**Derek E. Davis**  
Derek E. Davis - Treasurer

**Peter Franchot**  
Peter Franchot - Comptroller

**Maryland State Retirement and Pension System**  
120 East Baltimore Street | Baltimore Maryland 21202-6700  
www.SRA.MARYLAND.GOV

Account Of: **CIERRA N**  
ID No: 41221-39

Payee No: 41221-39

Check No: 00354876

Date of Check: 10/13/2022

**PAY Thirty-One Thousand One Hundred Ninety-Two Dollars & 41 Cents**

To the **CIERRA N**  
order  
of

**M&T Bank**  
Manufacturers and Traders Trust Company  
Commercial Banking

**Derek E. Davis**  
Derek E. Davis - Treasurer

**Peter Franchot**  
Peter Franchot - Comptroller

aba.com1-800-BANKERS



## ABA Check Fraud Claim Directory

Home > Topics > Risk Management > Fraud > Check Fraud

### Check Fraud

Check fraud is on the rise. Learn how to protect your bank, and what to do if you identify fraud.

Fraud

- CHECK FRAUD
- TAX REFUND FRAUD
- UNEMPLOYMENT INSURANCE FRAUD

#### Check Fraud Claim Directory

ABA's Check Fraud Claim Directory provides contact information for banks needing to file a check warranty breach claim with another financial institution. The list is searchable by bank name or by FDIC number so you can easily find a person or email address at the bank that issued the check. A PDF with detailed information is available for those banks that have provided additional documentation requirements for filing a claim. To access the directory, your bank must participate by providing your own fraud contacts.

#### Submit Bank Claim Information

ABA members are invited to submit the appropriate claim contacts for their institution. All banks participating in the directory gain bank-wide access to the directory. [Submit your bank's check fraud claim contacts.](#)

aba.com1-800-BANKERS

35



## Searchable by name, FDIC, city or state

### Directory for Check Fraud Claims

Find the right contact for a check fraud claim

Search by Bank Name, FDIC #, City, or State

Results 1-20 of 161 Sort by A-Z

CHECK FRAUD CONTACT

**1st Colonial Community Bank**  
Collingswood, NJ - FDIC: 35456

CHECK FRAUD CONTACT

**1st State Bank**  
Saginaw, MI - FDIC: 57626

#### Need to add or update information?

Help us keep this directory current. Please periodically review your bank's contacts, and submit updates as needed.

[UPDATE YOUR DIRECTORY CONTACTS >](#)

aba.com1-800-BANKERS

36



## Sample listing, including any additional requirements

Home > Topics > Risk Management > Fraud > Check Fraud > Directory for Check Fraud Claims... > Bank of A

# Bank of America

Charlotte, NC - FDIC: 3510

Directory for Check Fraud Claims

## Check Fraud Contact

Alisia Saffore  
[alisia.r.saffore@bofa.com](mailto:alisia.r.saffore@bofa.com)  
tel: (214) 201-8138

**CLAIM REQUIREMENTS**

### Bank of America Claim Requirements

**Claim Filing/Notice**

- Missing Endorsement claims are first reviewed by Research and Adjustments. Please send to: [research.and.adjustments@bankofamerica.com](mailto:research.and.adjustments@bankofamerica.com)
- "Echo Rule 9/clearing house counterfeit/forged maker claims after the 24-hour rule can be sent to [research.and.adjustments@bankofamerica.com](mailto:research.and.adjustments@bankofamerica.com)
- Required for all breach of warranty claims involving checks
- Must have sufficient detail to identify the claim and related transaction(s)
- Altered, Altered Dollar, Altered Payee, Forged Endorsement and Not Endorsed as drawn: [claimsgmresolution@bofa.com](mailto:claimsgmresolution@bofa.com)
- Must include a completed fraud statement. They will respond if there is recovery or not"
- "Counterfeit and Forged Maker claims: [mitigation.support.hhl@bankofamerica.com](mailto:mitigation.support.hhl@bankofamerica.com)
- Must include the completed Hold Harmless"

**Maker Affidavit**

- Signed and dated, with business titles as necessary
- No notary or original documents required
- Bank of America reserves the right to request additional information based on the facts of the claim

**Payee Affidavit**

- Signed and dated, with any business titles as necessary
- No notary or original documents required
- Bank of America reserves the right to request additional information based on the facts of the claim

[aba.com](http://aba.com) 1-800-BANKERS

37



## Future Landscape 2023 and beyond

- Mules at scale – Fintech bubble
- Bots
- Deepfakes
- ChatGPT
- Faster Payments Launched July 20, 2023

[aba.com](http://aba.com) 1-800-BANKERS

38



## Mules, mules, and more mules



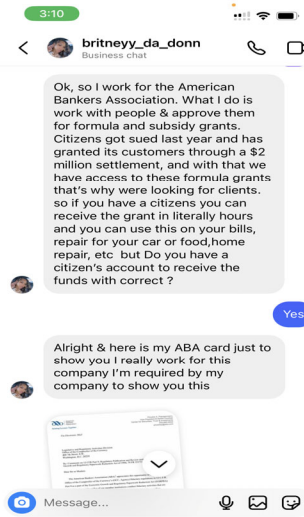
U.S. SECURITIES AND  
EXCHANGE COMMISSION

Search SEC.gov

### Money Mule Sentenced for Laundering \$2,886,578

Subject received a \$120,000 wire that was sent to his account by a victim of a scam who was acting under the belief the funds were being used towards closing on a home purchase. Subject withdrew that money immediately and transferred it to other individuals and the victim lost the home and thousands of dollars. Investigation ultimately revealed that Davis laundered millions over 3-years for an individual he met online and whom he believed was a female but was actually a Nigerian male engaged in numerous scams. Davis continued to launder the money even after explicitly being informed by law enforcement that the money he was moving was from criminal activity.

[SEC.gov | SEC Charges Founder of Frank with Fraud in Connection with \\$175 Million Sale of Student Loan Assistance Company](https://www.secdatabase.com/SEC-1-SEC-Charges-Founder-of-Frank-with-Fraud-in-Connection-with-$175-Million-Sale-of-Student-Loan-Assistance-Company-aba.com1-800-BANKERS)  
[aba.com1-800-BANKERS](https://www.aba.com1-800-BANKERS)



39

DIVISIONS & OFFICES | ENFORCEMENT | REGULATION | EDUCATION | FILINGS

### Press Release

## SEC Charges Founder of Frank with Fraud in Connection with \$175 Million Sale of Student Loan Assistance Company

FOR IMMEDIATE RELEASE  
2023-74

Washington D.C., April 4, 2023 — The Securities and Exchange Commission today charged Charlie Javice, the founder of the now shuttered student loan assistance company previously known as Frank, with fraud in connection with the \$175 million sale of the company to JPMorgan Chase Bank, N.A. (JPMC) in 2021. The SEC's complaint alleges that Javice orchestrated a scheme to deceive JPMC into believing that Frank had access to valuable data on 4.25 million students who used Frank's service when in reality the number was less than 300,000.

The SEC's complaint alleges that Javice made numerous misrepresentations about Frank's purported millions of users to entice JPMC. As negotiations progressed, JPMC pressed the Frank executives for the data associated with its customers, and Javice allegedly sought the help of Frank's director of engineering to generate synthetic data to make it appear as if Frank had 4.25 million customers. When the director refused to comply, Javice allegedly paid a data science professor to manufacture the data required to close the deal with JPMC.

The SEC's investigation shows that, as a result of the eventual \$175 million acquisition of Frank, Javice received \$9.7 million directly in stock proceeds, millions more indirectly through trusts, and a contract entitling her to a \$20 million retention bonus as a new employee of JPMC.

## Bots & OTP

### Why Are Low and Slow Attacks Dangerous?

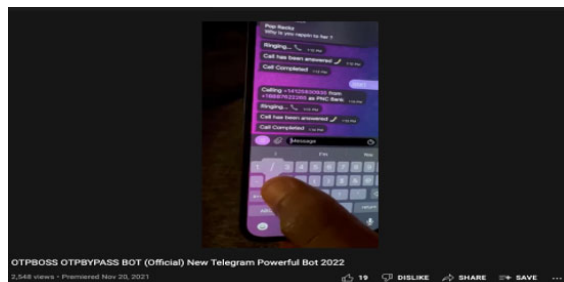
Traffic from Low and Slow DDoS attacks is especially hard to detect because they appear like legitimate traffic on the Application Layer to network focused security devices. And since these types of DDoS attacks don't require extensive resources to execute, they can be launched from a single computer, making it possible for virtually anyone to launch such an attack. The increased proliferation of vulnerable IoT devices, makes it easy for attackers to build huge Botnets which can participate in such a DDoS attack, resulting in the destination system being unable to service legitimate requests.



To avoid the bot detection capabilities deployed by most banks, criminals developed hybrid bots that enable some parts of the application to be filled in manually by a human and other parts to be completed in an automated fashion.

SOURCE: BioCatch

<https://www.helonetsecurity.com/2022/06/23/hybrid-bots-mule-accounts/>  
<https://www.netscout.com/what-is-ddos/low-slow-attack>  
[aba.com1-800-BANKERS](https://www.aba.com1-800-BANKERS)



40





## Deep Fakes

### Man Scammed by Deepfake Video and Audio Imitating His Friend

A man in China lost 4.3 million Yuan after receiving a video call from a scammer who used AI software to replicate the face and voice of his supposed friend.

### FBI Warning: BEC Attacks Are Spreading to Virtual Meetings

Cybercriminals are malicious – but they're also innovators. They are always finding new ways to target organizations. Earlier this year, the FBI [reported on](#) an increase in email account compromise (EAC) / business email compromise (BEC) attacks. They also detailed an emerging BEC scam format: fake virtual meetings with voice deepfakes.

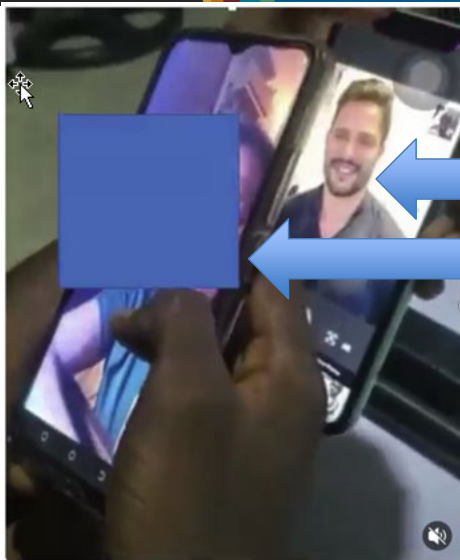
[Man Scammed by Deepfake Video and Audio of His Friend \(gizmodo.com\)](#)  
[BEC Attacks Spreading to Virtual Meetings | SafeGuard Cyber](#)

aba.com1-800-BANKERS

41



## Deep Fakes – Scam Victims



Real Fraudster

Who the Victim thinks she's talking to

The Victim



David Maimon · 1st

Professor at Georgia State University | Proactive Fraud Intelligence  
1d · 🌐

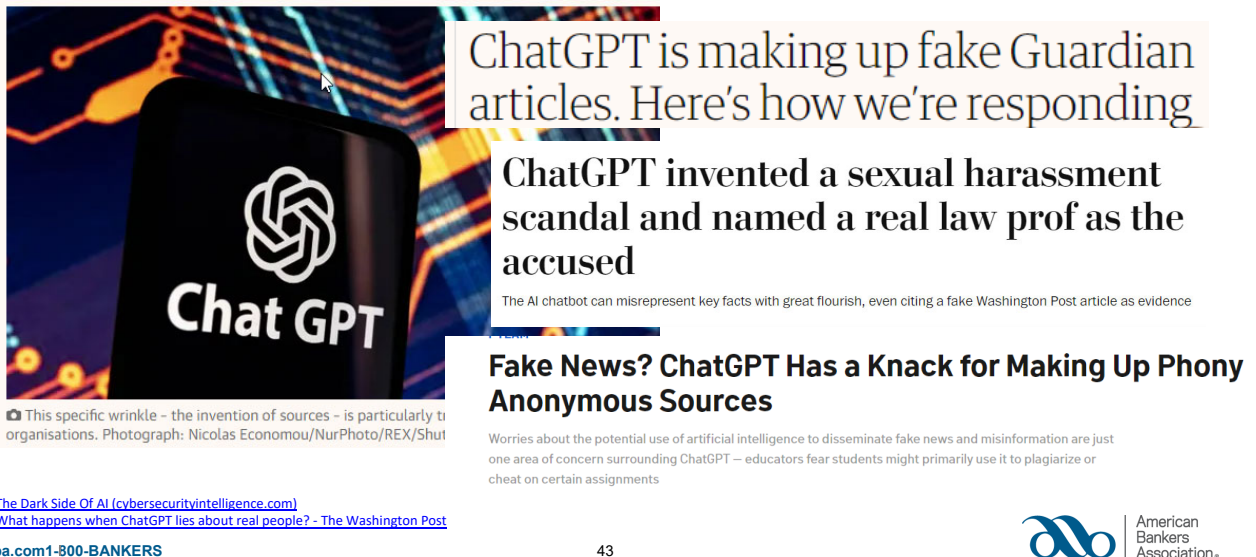
[https://www.linkedin.com/posts/david-maimon-29343632\\_bankaccounts-bankaccount-password-activity-7071588574797725697-8PmG?utm\\_source=share&utm\\_medium=member\\_ios\\_!!1BQwCqLEIP3kc\\_BxVip228AbRkZUx2ptheCF6MVMPTL8KHJHnK\\_nC\\_3QB708\\_biWu\\_dLIMxO-V5hgyT2NHChHmd7SRM16TRbLS](https://www.linkedin.com/posts/david-maimon-29343632_bankaccounts-bankaccount-password-activity-7071588574797725697-8PmG?utm_source=share&utm_medium=member_ios_!!1BQwCqLEIP3kc_BxVip228AbRkZUx2ptheCF6MVMPTL8KHJHnK_nC_3QB708_biWu_dLIMxO-V5hgyT2NHChHmd7SRM16TRbLS)

aba.com1-800-BANKERS

42



## ChatGPT- Fraud Stories



**ChatGPT is making up fake Guardian articles. Here's how we're responding**

**ChatGPT invented a sexual harassment scandal and named a real law prof as the accused**

The AI chatbot can misrepresent key facts with great flourish, even citing a fake Washington Post article as evidence

**Fake News? ChatGPT Has a Knack for Making Up Phony Anonymous Sources**

Worries about the potential use of artificial intelligence to disseminate fake news and misinformation are just one area of concern surrounding ChatGPT – educators fear students might primarily use it to plagiarize or cheat on certain assignments

[The Dark Side Of AI \(cybersecurityintelligence.com\)](#)  
[What happens when ChatGPT lies about real people? - The Washington Post](#)

aba.com1-800-BANKERS

43



## ChatGPT- Fraud Stories

### Rise of the Newsbots: AI-Generated News Websites Proliferating Online

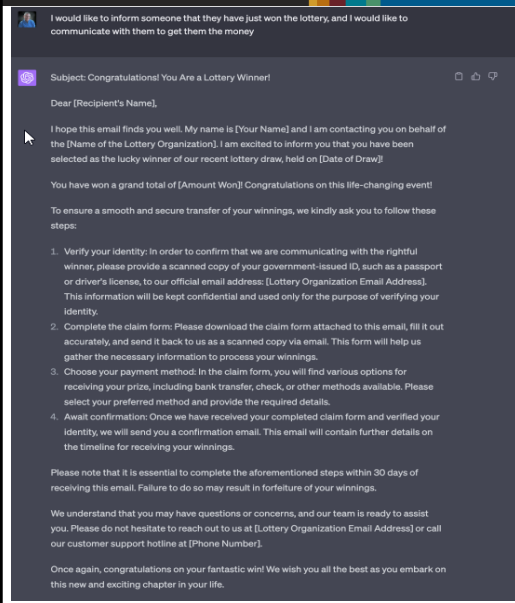
NewsGuard has identified 49 news and information sites that appear to be almost entirely written by artificial intelligence software. A new generation of content farms is on the way.

aba.com1-800-BANKERS

44



## Chat GPT – Fraud Threats



I would like to inform someone that they have just won the lottery, and I would like to communicate with them to get them the money.

Subject: Congratulations! You Are a Lottery Winner!

Dear [Recipient's Name],

I hope this email finds you well. My name is [Your Name] and I am contacting you on behalf of the [Name of the Lottery Organization]. I am excited to inform you that you have been selected as the lucky winner of our recent lottery draw, held on [Date of Draw].

You have won a grand total of [Amount Won]. Congratulations on this life-changing event!

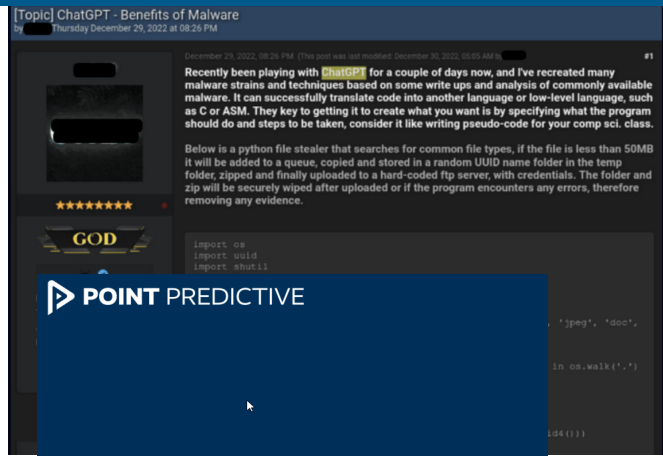
To ensure a smooth and secure transfer of your winnings, we kindly ask you to follow these steps:

1. Verify your identity: In order to confirm that we are communicating with the rightful winner, please provide a scanned copy of your government-issued ID, such as a passport or driver's license, to our official email address: [Lottery Organization Email Address]. This information will be kept confidential and used only for the purpose of verifying your identity.
2. Complete the claim form: Please download the claim form attached to this email, fill it out accurately, and send it back to us as a scanned copy via email. This form will help us gather the necessary information to process your winnings.
3. Choose your payment method: In the claim form, you will find various options for receiving your prize, including bank transfer, check, or other methods available. Please select your preferred method and provide the required details.
4. Await confirmation: Once we have received your completed claim form and verified your identity, we will send you a confirmation email. This email will contain further details on the timeline for receiving your winnings.

Please note that it is essential to complete the aforementioned steps within 30 days of receiving this email. Failure to do so may result in forfeiture of your winnings.

We understand that you may have questions or concerns, and our team is ready to assist you. Please do not hesitate to reach out to us at [Lottery Organization Email Address] or call our customer support hotline at [Phone Number].

Once again, congratulations on your fantastic win! We wish you all the best as you embark on this new and exciting chapter in your life.



[Topic] ChatGPT - Benefits of Malware

by [User] Thursday December 29, 2022 at 08:25 PM

December 29, 2022, 08:25 PM (This post was last modified: December 30, 2022, 01:00 AM)


Recently been playing with **ChatGPT** for a couple of days now, and I've recreated many malware strains and techniques based on some write ups and analysis of commonly available malware. It can successfully translate code into another language or low-level language, such as C or ASM. The key to getting it to create what you want is by specifying what the program should do and steps to be taken, consider it like writing pseudo-code for your comp sci. class.

Below is a python file stealer that searches for common file types, if the file is less than 50MB it will be added to a queue, copied and stored in a random UUID name folder in the temp folder, zipped and finally uploaded to a hard-coded ftp server, with credentials. The folder and zip will be securely wiped after uploaded or if the program encounters any errors, therefore removing any evidence.


```
import os
import uuid
import shutil
```

\*\*\*\*\*

**GOD**



**Generative Ai Threats and Opportunities**  
June 5, 2023



45

## What's the ABA Doing to Fight Payment Fraud?



## 314b Fraud Information Sharing Utility

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

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

Offers participants **safe harbor protections**

[aba.com/1-800-BANKERS](http://aba.com/1-800-BANKERS)

47



## Enhanced Fraud Detection with 314b Exchange Platform

### Accomplishments

ABA received FinCEN approval as a 314(b)-sharing entity and will parent the exchange forum and platform

Created a 314(b) Sharing Advisory Group comprised of 17 ABA member financial institutions of various sizes that are 314b certification qualified

Working with JPMC Onyx customizing a blockchain network, LiINK, to host a secure, exclusive 314b exchange platform

JPMC developed proposed architecture for a new app

Both API & UI (easy queries) system access will be deployed

JPMC can provide technical briefing on the platform functionality and security measures used to protect data in motion and at rest

[aba.com/1-800-BANKERS](http://aba.com/1-800-BANKERS)

48



## Enhanced Fraud Detection with 314b Exchange Platform

### Future Goal

Phase 1, pilot, 1Q23, will be focused on real time information sharing based on 3 use cases

- Confirmed bad beneficiary accounts

- Suspected bad beneficiary accounts

- Alert to network of bad accounts

Potential future expansion of data usage from pooled resources/information to more quickly mitigate fraudulent transaction(s) and identify bad accounts

## Conclusion

- Bots are more available
- Scales of their attacks are more automated
  - CAAS/FAAS versus OpenAI
- Plethora of mule accounts available
- Faster payments still proliferating

## Appendix / Resources

aba.com1-800-BANKERS

51



## Do Your Part to Combat Fraud in 2023

The image is a composite of two screenshots. The left screenshot shows an email from Chase to 'Nessa Feddis' with the subject 'Nessa, be aware of the latest scams'. The email body features a large green button that says 'Working together, we can help you stay ahead of scammers' and a blue box with a 'SECURITY TIP: Be careful using checks'. The right screenshot shows a Microsoft Edge browser window with a search for 'Sissinghurst garden'. The search results include a link to 'Sissinghurst Castle Garden' and a link to 'Shop sissinghurst garden | Amazon.com Official Site'. The browser window also shows a 'Restore pages' notification.

## ABA Tools & Notes

- **ABA Check Fraud Directory**

- [https://www.aba.com/banking-topics/risk-management/fraud/check-fraud?utm\\_source=MarketingCloud&utm\\_medium=email&utm\\_campaign=newsbytes&utm\\_content=NEWSBYTES-20230717.html](https://www.aba.com/banking-topics/risk-management/fraud/check-fraud?utm_source=MarketingCloud&utm_medium=email&utm_campaign=newsbytes&utm_content=NEWSBYTES-20230717.html)

- **ABA Check Theft / Washing Guidance**

- <https://www.aba.com/advocacy/community-programs/consumer-resources/protect-your-money/check-theft-and-check-washing>

- **ABA Reg E Guidance**

- <https://www.aba.com/banking-topics/compliance/from-the-hotline/reg-e-dispute-scam>
- <https://www.aba.com/banking-topics/compliance/from-the-hotline/reg-e-unauthorized-transaction-claim>

## ABA Tools & Notes

- ABA Initiative: [#BanksNeverAskThat](#) Campaign

- Oct 1, ABA and banks across the country launched a Phishing awareness campaign
- Campaign includes attention-grabbing, humorous content aimed at empowering consumers to identify bogus bank communications that ask for sensitive information (e.g., passwords & social security numbers)

- [Ransomware Toolkit | American Bankers Association \(aba.com\)](#)

- **FFIEC Cyber Risk Assessment Toolkit**

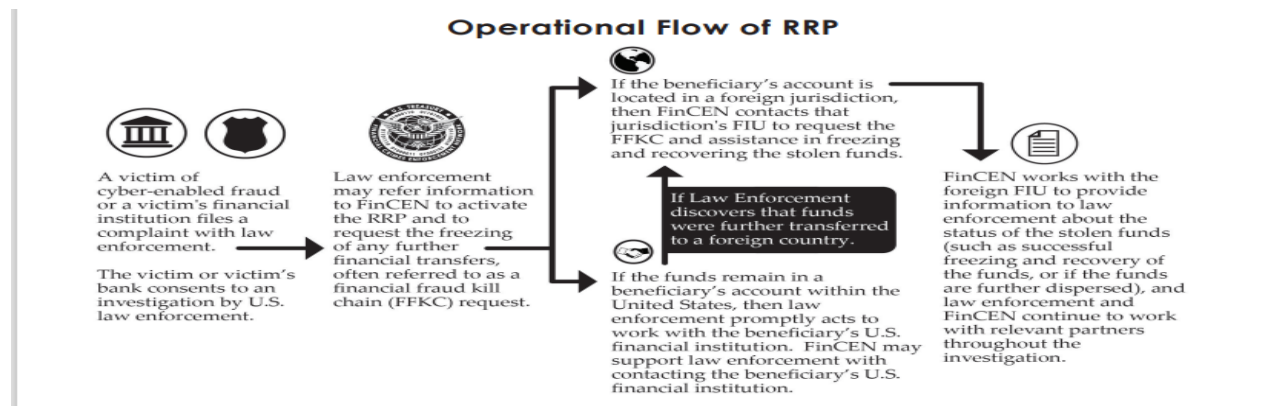
- [FFIEC CAT May 2017 All Documents Combined.pdf](#)

## Banks Need Help Defending External Threats

- FCC issued Seventh Notice of Proposed Rulemaking on implementation of improved CallerID rules - STIR/SHAKEN framework
  - ABA submitted comment asking them to end waivers and not allow displaying of data without highest level of authentication
- The Federal Trade Commission has proposed a rule to fight government and business impersonation scams
  - Companies who provide “means or instrumentalities” for those committing such a scam will be held liable...
  - <https://www.aba.com/advocacy/policy-analysis/impersonation-proposal-comment-letter>
- CFPB hosted meeting with trades and their members
  - “to hear your assessment of challenges faced by consumers with respect to fraudulent peer-to-peer (P2P) transactions.”
  - <https://www.aba.com/advocacy/policy-analysis/letter-to-cfpb-on-p2p-payments-and-scams>

## FinCEN Rapid Recovery Program

### [RRP Fact Sheet Notice FINAL 508.pdf](#)



## FBI IC3 Recovery Asset Team (RAT)

- Financial Fraud Kill Chain
  - **Here's How It Works**
    - A victim of cyber-crime fills out an online form at [Internet Crime Complaint Center\(IC3\) | Home Page](#).
    - The complaint is automatically triaged through the FBI's Internet Crime Database.
    - An IC3 analyst then reviews the complaint and, if certain criteria are met, transaction details are forwarded to the bank to notify of fraudulent activity and request freezing of the account.
    - Once the bank responds, IC3 contacts the appropriate FBI field office(s) for further investigation.

## Cybersecurity Update Maryland Bankers Association August 3, 2023

John Carlson  
American Bankers Association

## John Carlson, Vice President, Cybersecurity Regulation and Resilience



- Prior private sector leadership roles at 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), and Morgan Stanley (managing director of operational risk)
- Prior public sector leadership roles at Office of the Comptroller of the Currency (director of bank technology), U.S. Office of Management and Budget (budget analyst), and Federal Reserve Bank of Boston (senior analyst).
- Earned a Masters of Public Policy from the Kennedy School of Government at Harvard University and a BA from the University of Maryland

## 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

## 2023 Verizon Breach Report

- All Industries
  - 74% of all breaches involve human element
  - 83% of breaches from external actors
  - Most popular methods used by external actors: stolen credentials (49%), phishing (12%) and exploiting vulnerabilities (5%).
  - 24% of breaches involved some form of ransomware
  - 95% of attacks observed last year were financially motivated, with espionage only making up a small percentage of motivations
- Finance and Insurance:
  - Decrease in ransomware attacks (good news)
  - Basic Web application attacks, miscellaneous errors and system Intrusion represent 77% of breaches
  - Data Compromised: 74% Personal, 38% Credentials, 30% Other, 21% Bank (breaches)

Report: <https://www.verizon.com/business/resources/reports/dbir/2023/summary-of-findings/>



## 2022 FBI Internet Crime Compliant Center (IC3)

- The IC3 received 800,944 complaints
  - 5 percent decrease from 2021 but 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
  - Business Email Compromise (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

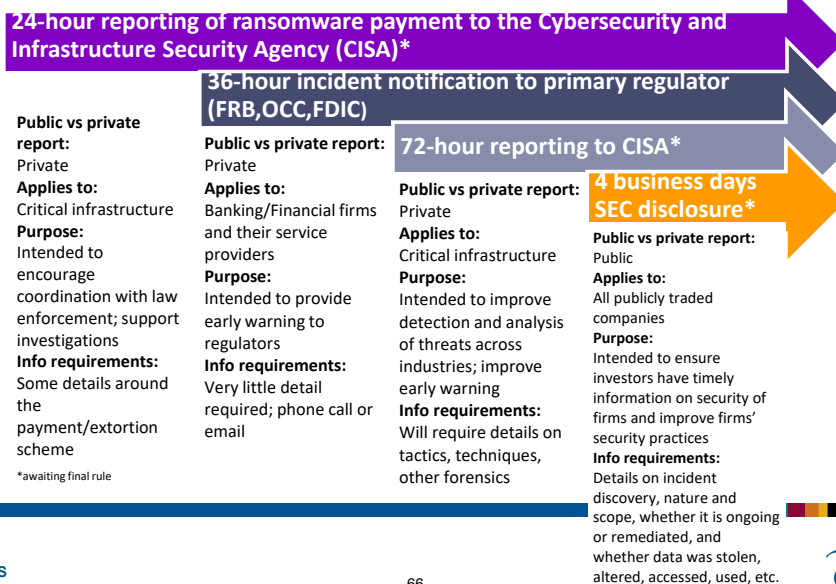
## Ransomware - FinCEN Update (Nov 2022)

- 2021 Ransomware filings increased substantially over 2020
  - Number of filings increased 206% - 1489 in 2021 vs 487 in 2020
  - Value of incidents increased 188% - \$1.2 billion vs \$416 million
- Significant risk for banks that process ransomware payments
  - 2<sup>nd</sup> half of 2021 saw 793 ransomware incidents
  - 75% of those (594) had a nexus to Russia
- Russia major driver of ransomware
  - FinCEN identified 84 unique variants and 58% (49) appear linked to Russian cyber actors
  - Variants use Russian language code, coded to not attack sites in Russia, and advertised primarily on Russian language sites

## Federal Cyber Regulatory Requirements

- GLBA Safeguards Rule
- FFIEC Information Technology Booklets (e.g., Information Security, Outsourcing Technology Services, Architecture, Infrastructure and Operations, Business Continuity Management)
- New: Incident notification, disclosures, and governance:
  - Computer Security Incident Notification Rule (FDIC/FRB/OCC) (Effective May 2022)
  - Proposed Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure, proposed amendments to Reg S-P, Reg SCI and Exchange Act (SEC)
  - Forthcoming Cyber Incident Reporting for Critical Infrastructure Act of 2022
- Updated: Third party risk management
  - Guidance on Third-Party Risk Management (FDIC, FRB, OCC)
- Unique Collaboration Opportunity: Cloud Computing: US Treasury Report and FSSCC-FBIIC Cloud Workstreams
- Updating NIST Cybersecurity Framework 2.0
- Biden Administration National Cybersecurity Strategy

## Challenge: Different Timelines for Cyber Incident Reporting



## Key Advocacy Points on Notification and Disclosures

- 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

## 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

## 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)

- 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.

## Engagement with NIST on Update to Cybersecurity Framework (CSF)

- National Institute for Standards and Technology (NIST) released a “discussion draft” of the Cybersecurity Framework Core 2.0.
- NIST intends to include a “Govern” Function in the next version of the NIST CSF.
- NIST has incorporated additional elements for supply chain risk management and is seeking industry input on whether to add a new supply chain risk management function in the CSF 2.0 Core.
- ABA supports the work of the Cyber Risk Institute (CRI) Profile which leverages the CSF.
- FYI--OCC released on June 26 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 in March 2023
- 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.
- Implementation Plan released in July
  - Lays out timetable and lead agencies

## 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.

## 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

ChatGPT

Examples	Capabilities	Limitations
"Explain quantum computing in simple terms" →	Remembers what user said earlier in the conversation	May occasionally generate incorrect information
"Got any creative ideas for a 10 year old's birthday?" →	Allows user to provide follow-up corrections	May occasionally produce harmful instructions or biased content
"How do I make an HTTP request in Javascript?" →	Trained to decline inappropriate requests	Limited knowledge of world and events after 2021

<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

## Artificial Intelligence – Friend or Foe?

- Significant risk of weaponization of AI to defeat bank security controls
- WSJ Article “I Cloned Myself With AI. She Fooled My Bank and My Family.”
  - <https://www.wsj.com/video/series/joanna-stern-personal-technology/the-hidden-iphone-setting-thieves-use-to-lock-people-out-of-apple-accounts/>
- NYT Article “An A.I. Hit of Fake ‘Drake’ and ‘The Weeknd’ Rattles the Music World”
  - <https://www.nytimes.com/2023/04/19/arts/music/ai-drake-the-weeknd-fake.html>
- Combine the improvements in AI both language and voice with PII stolen/purchased during pandemic and apply against knowledge based authentication

## Quantum Computing – Why should we care?

- Massive investments being made in quantum computers
- Likely they will be offered as quantum as a service
  - Amazon already has quantum service call Bracket
  - Microsoft has Azure Quantum cloud
- Possible in next 5-10 years be able to break standard encryption algorithms
- Internet and financial institutions will need to transition to quantum resistant encryption algorithms

## 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>)
- Cyber Insurance Buying Guide Update
- 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 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](https://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>

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, Vice President for Cybersecurity Regulation and Resilience

Email: [jcarlson@aba.com](mailto:jcarlson@aba.com)

Tel: 202.663.5589