

150 YEARS  
1875-2025



American  
Bankers  
Association®

# Furthering the Fight Against Check Fraud

---

NAST



**Jim Hitchcock**  
**Vice President, Fraud Mitigation**  
**American Bankers Association**  
**[jhitchcock@aba.com](mailto:jhitchcock@aba.com)**

Jim serves as the association's primary expert on fraud mitigation activities and programs. In this role, he identifies and tracks key fraud topics and trends, develops fraud prevention strategies, and finds opportunities to develop capabilities and partnerships that provide products and services to banks. Prior to joining ABA during June 2021, Jim was a Director in the Capital One Anti-Money Laundering Department serving in a Fraud Advisory role. Jim began his banking journey during February 2016 after a career in Federal law enforcement with the U.S. Department of Defense Inspector General (Investigations) and U.S. Secret Service.

DISCLAIMER

THIS PRESENTATION IS FOR EDUCATIONAL AND INFORMATIONAL PURPOSES ONLY. IT IS PRESENTED WITH THE UNDERSTANDING THAT THE PRESENTER IS NOT PROVIDING YOU WITH LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF YOU REQUIRE LEGAL ADVICE OR OTHER EXPERT ASSISTANCE, YOU SHOULD SEEK THE SERVICES OF A COMPETENT PROFESSIONAL.

- Check Fraud, Oldest Crime isn't Going Away
- Check Liability & Recovery
- Oldest Crime Meets Newest Technology
- Synthetic Business Accounts
- What's ABA Doing to Continue the Fight

# Good Ole CHECK FRAUD

From NYT 1920

“Do you know the methods of the mailbox thieves who have recently renewed operations here in New York?”

← SUBJECTS

## “SCRATCHING” CHECKS.

Warning to Public of New Methods of Fraud  
—Banks Limit of Responsibility.

DO you leave your check book carelessly around your desk, where it is accessible to any one? Do you know who is responsible, you or the bank, if you lose an indorsed check in the street and a bank cashes it on the strength of your indorsement? Do you know about the counter indorsement trick? Do you know the methods of the mail box thieves, who have recently renewed operations here in New York?

CONTINUE READING: PDF

PUBLISH DATE

October 31, 1920

PAGE NUMBER

113

SUBJECTS

Burns Internatl Detective Agency

## “SCRATCHING” CHECKS.

Warning to Public of New  
Methods of Fraud—Banks  
Limit of Responsibility.

DO you leave your check book carelessly around your desk, where it is accessible to any one? Do you know who is responsible, you or the bank, if you lose an indorsed check in the street and a bank cashes it on the strength of your indorsement? Do you know about the counter indorsement trick? Do you know the methods of the mail box thieves, who have recently renewed operations here in New York?

The whole question of check procedure has been discussed over and over again. Banks have issued warnings and books of advice to new depositors in regard to the care they should take of their checks and the general responsibility of individuals and banks in regard to a checking account. In spite of all this warning, stolen checks, forged, raised and worthless checks continue to be presented at banks for payment, and banks continue to honor them. Until something happens to an individual's check or until some spectacular case comes up the average person forgets the risks of checks and only remembers the conveniences. The case now under litigation of Mrs. O. H. P. Belmont vs. the Central Union Trust Company in regard to raised or forged checks has brought the matter again before the public eye.

A bank official of a large downtown bank, in discussing the whole raised-check, forged-check situation in general, said: “Fortunately no one bank has a great many of these to deal with, but putting all the banks together, of course frauds are being perpetrated and attempted all the time. As a general thing you will not find banks having any disposition to evade their responsibilities. The whole banking business is built on confidence and banks do not endeavor to shift the responsibilities that come with confidence. However, if it can be shown that the depositor has not used ordinary caution about checks, has been in the habit of signing blank checks and turning them over to some other person to fill in—well, that is a question of law rather than rule-of-thumb banking.

“People should learn not to leave check books about. Even the printers who make check books for banks are supposed to use great care in handling the proof sheets. Women should also learn to begin writing in their figures as far over to the left hand side as

# White House Executive Order Phasing Out Treasury Paper Checks

- Effective September 30, 2025, the Federal government will cease issuing paper checks for all disbursements, including intragovernmental payments, benefits, vendor payments, and tax refunds.
- Payments made to the Federal government, such as fees, fines, loans, and taxes, must also be processed electronically where permissible under existing law.
- **Exceptions** *will be made for people without banking or electronic payment access*, certain emergency payments, certain law enforcement activities, and other special cases qualifying for an exception under the Order or other existing law.

**Presidential Executive Order For  
\$5,000 Stimulus Checks?**

**ACH or CHECK?**



## Wire

- Scam Incident Rate – 6.35%
- Average Scam Claim – \$30,357.73

## Bill Pay

- Scam Incident Rate – 0.45%
- Average Scam Claim – \$11,016.54

## Zelle

- Scam Incident Rate – 14.40%
- Average Scam Claim – \$1,892.96

## Transfers

- Scam Incident Rate – 5.80%
- Average Scam Claim – \$23,117.31

## Cash Withdrawal

- Scam Incident Rate – 15.70%
- Average Scam Claim – \$12,381.73

## Check Inclearing

- Scam Incident Rate – 20.03%
- Average Scam Claim – \$35,730.17

## Debit Cards

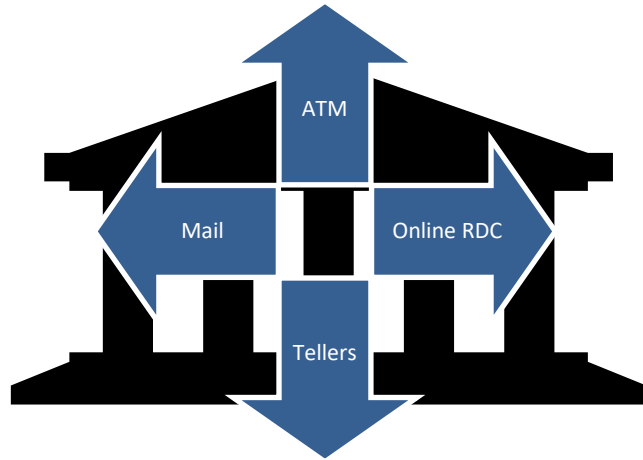
- Scam Incident Rate – 32.37%
- Average Scam Claim – \$4,799.75

# CHECKS – Inherently Risky

- Risk: A check has weak internal security
  - Check stock
  - Signature
  - MICR line
- Risk: Check deposit processes are subject to error. The true intent of the check is not evident until after the check has cleared and the client responds.
- Risk: Check funds recovery processes are subject to individual bank interpretations of the regulations and terms.



## ✓ Deposits (ATM / Branch)



## X Remote Deposit Capture (RDC)

- Regulation CC imposes funds availability requirements on checks, electronic payments, and cash. Checks deposited through a mobile device are not any of these.
- Regulation CC's §1029.2(k)(1) defines a "check" as "a negotiable demand draft drawn on or payable through or at an office of a bank."
  - A picture of a check that a customer transmits to the bank using the customer's mobile device is not "negotiable" and therefore not a check under Regulation CC's definition of the term.
- Nor is such an item an "electronic payment" under Regulation CC, which it defines as "a wire transfer or an automated clearing house (ACH) credit transfer."
- Banks MAY nevertheless apply their standard funds availability policy to such deposits.
- **Fraud Exception:** When we have "reasonable cause" to doubt collectability of a check deposited, Reg CC may allow us to delay availability of the funds by placing a hold on the check. Reasonable cause requires the existence of facts that would cause a well-grounded belief in the mind of a reasonable person that the check is uncollectible from the paying bank.

✓ Reg CC generally requires deposits to be available within 1-2 business days, but allows exceptions...

## Next Day Availability (7/1/25 \$275)

NEXT DAY ITEMS		
<ul style="list-style-type: none"> <li>♦ Cash</li> <li>♦ Electronic payments: Wires, ACH</li> <li>♦ (ACH available same day under NACHA rule)</li> <li>♦ U.S. Treasury Checks</li> <li>♦ U.S. Postal Service Money Orders</li> <li>♦ State or Local Government Checks</li> </ul>	<ul style="list-style-type: none"> <li>♦ Cashier's Checks</li> <li>♦ Certified Checks</li> <li>♦ Teller's Checks</li> <li>♦ "On-Us" Checks</li> <li>♦ Federal Reserve Bank Checks</li> <li>♦ Federal Home Loan Bank Checks</li> </ul>	
LOCAL CHECKS*	Case-by-Case Hold Period	Exception Hold Period
Banks in same "region"	2 Business Days (Funds must be available for withdrawal no later than the 2 <sup>nd</sup> business day following the banking day of deposit)	7 Business Days (Funds must be available for withdrawal no later than the 7 <sup>th</sup> business day following the banking day of deposit)

## Exceptions to Reg CC

New Accounts	Account 30 days or less unless customer has another older account with bank
Large Deposits	>= \$5,525, any single banking day. Only portion of funds are available within timeframes
Redeposited Items	As long as not originally endorsed or post date and post date is current
Repeated Overdrafts	For at least 6 days in last 6 months OR a negative balance of \$5,525 for at least 2 days over 6 months
Reasonable Doubt	Facts that would cause a well-grounded belief in the mind of a reasonable person that the check is uncollectible.
Emergency	Natural disasters, comm interruptions, a situation that prevents the bank from processing checks normally.

# The Ever-Present Challenge

**Altered Check** : Unauthorized change in the check that modifies the obligation of the party, typically payee and/or amount

**Forged Endorsement** : Jane's signature was forged, the payee of the item, on the back of the check

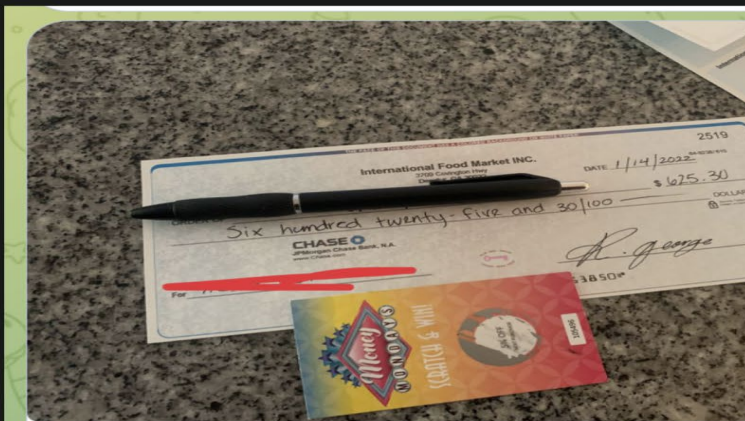
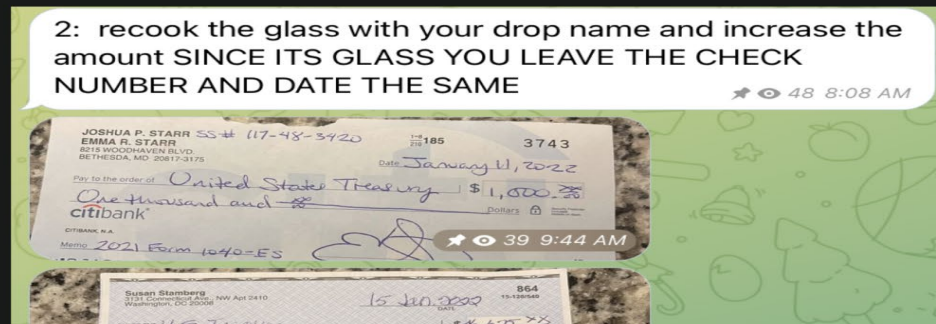
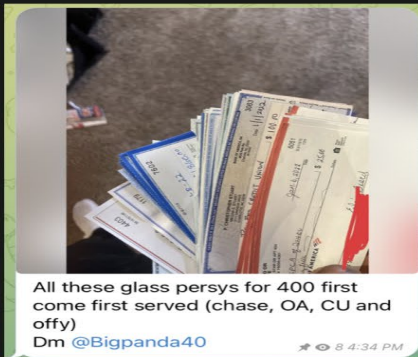
**Counterfeit**: a check with a forged or unauthorized drawer signature. Typically fabricated by compromised routing/account number

**Forged Maker Signature** : Sam's signature was forged, the maker on the front of the check

Fraud Type	BOFD Liable	Paying Bank is Liable	Timeframe for Liability
Altered Check	X		1 year from date of deposit
Forged Endorsement	X		3 years from date of deposit
Forged Maker Signature		X	1 day after presenting for payment
Counterfeit		x	1 day after presenting for payment

# Bigger Challenges

## Fresh Glass - These Checks Are Guaranteed To Clear



## CHECK COOKING LESSONS

Comes with :

- Check Software (No download required) Must have laptop or PC
- How to Wash Personal Checks and how to stretch 🔥 and tools included
- 1 on 1 intro to check learn transit number, the difference between biz persy and offy
- starter grub included
- Learn what accounts pop on what
- Learn what hold's and credit and debits are
- Learn about how to choose and target Drop accounts



# Fraud-As-A-Service: Drops on Drops (Mules 2.0)



## New Fullz

- Name
- Address
- Bank Acct
- Seasoned Funds
- Seasoned Device

## Threats

- Bypasses Device Profiling
- Bypasses Typical Mule profiling

## Solutions

- Transactional Behavior
- Fusion type Fraud Strategy



FINANCIAL CRIMES ENFORCEMENT NETWORK

# Financial Trend Analysis

Mail Theft-Related Check Fraud:  
Threat Pattern & Trend Information,  
**February to August 2023**

September 2024

## EIN Assistant

Your Progress: 1. Identity ✓ 2. Authenticate ✓ 3. Address

Congratulations! Your EIN has been successfully assigned.

EIN Assigned: 99-  
Legal Name: [REDACTED]

### IMPORTANT:

Save and/or print this page and the confirmation letter below for your permanent record. The confirmation letter below is your official IRS notice and contains important information about your new EIN.

[CLICK HERE for Your EIN Confirmation Letter](#) [Help with saving or printing your letter](#)

Once you have saved or printed your letter, click "Continue" to get additional information about using your new EIN.

[IRS Privacy Policy](#) [Accessibility](#)

Level up your hustle! Secure Funding and your LLC with CPN integration and IRS registration – just \$400

EIN LOOK UP AVAILABLE TOO

## FINANCIAL TREND ANALYSIS

### Sophisticated Methodologies

- **New account fraud:** New account fraud involved criminals opening new accounts, typically online, specifically designed to negotiate stolen checks.<sup>21</sup> This most frequently occurred when stolen checks were made out to businesses. Some criminals opened accounts either in the name of the payee or a name that is nearly identical. The company that opened the account may not actually exist and may use a fraudulent address during the account opening process. Perpetrators may open these accounts using compromised identifying information or synthetic IDs comprising of information from several people.
- **Mail theft-related check fraud as part of a larger scam, mostly romance and employment scams:** In these cases, scammers engaged victims in a scam and convinced them to negotiate a check and then send the funds elsewhere, using the victims as money mules to move stolen funds.
- **Insider involvement:** Sophisticated operations have enlisted insider assistance at financial institutions or the USPS.<sup>22</sup> In one case, federal prosecutors charged a USPS employee with stealing more than \$1.6 million in checks from the U.S. mail, altering the checks, and depositing them into his own account.<sup>23</sup>

NEWS • PRESS RELEASES

## D.A. Bragg: Check Fraud Ring Indicted For Stealing \$1.2M From Bazooka Companies, Maker Of Classic Bubble Gum

OCTOBER 3, 2024

Manhattan District Attorney Alvin L. Bragg, Jr., today announced the indictment of KASHAWN WILLIAMS, 31, for intercepting a \$1.2 million check intended for The Bazooka Companies Inc. ("Bazooka") and, alongside co-conspirators ADREAN JACOBS, 41, RONALD FRANKLIN, 49, JOSE GUTIERREZ, 25, AKHEIM WATTS, 30, and KIEARRA REYNOLDS, 35, laundering those stolen funds for personal use. The defendants are charged in a New York State Supreme Court indictment with Conspiracy in the Fourth Degree, Money Laundering in the First Degree, and Criminal Possession of Stolen Property in the First Degree, as well as various counts of Criminal Possession of Stolen Property in the Second Degree and Money Laundering in the Second and/or Third Degree. WILLIAMS is additionally charged with Grand Larceny in the First Degree and Identity Theft in the First Degree.<sup>[1]</sup>

"As alleged, this group stole more than a million dollars by intercepting a check, creating a fraudulent corporate business account, and laundering the money for personal gain," said District Attorney Bragg. "Despite the decline in the use of paper checks, check fraud is on the rise. We urge New Yorkers and businesses alike to use secure electronic payment methods whenever possible to protect themselves from fraud."

According to court documents and statements made on the record in court, in October 2022, WILLIAMS intercepted a \$1,243,345.36 check mailed by a Texas-based company to a Manhattan address formerly associated with Bazooka, the creators of the Bazooka brand of bubble gum. On October 21, 2022, WILLIAMS incorporated a fictitious entity – The Bazooka Companies 1 Inc. ("Bazooka 1") – to serve as a conduit for the stolen proceeds. Three days later, WILLIAMS opened a corporate bank account for Bazooka 1 and deposited the stolen check.

Over the course of the next two weeks, WILLIAMS issued checks from the Bazooka 1 account to JACOBS, WATTS, GUTIERREZ, and REYNOLDS, listing fake reasons for the checks on their memo lines, such as "Renovations," "Business Loan," and "Packaging Preorder." The defendants then deposited these checks into their personal bank accounts and made large cash withdrawals.

# Corporate Headquarters – KYC / KYB?



# KYC Passed

<https://apps.dos.ny.gov/publicInquiry/#search>

## Latest Filing Information

<b>Filing Number</b>	221021003171
<b>Filing Type</b>	CERTIFICATE OF INCORPORATION
<b>Mod Cert Code</b>	01DB A
<b>Approved Date</b>	2022-10-21
<b>Filing Date</b>	2022-10-21
<b>Entity Type</b>	DOMESTIC BUSINESS CORPORATION
<b>Current Entity Name</b>	THE BAZOOKA COMPANIES 0 INC.
<b>Effective Date</b>	2022-10-21
<b>Duration</b>	PERPETUAL
<b>Law Section</b>	BUSINESS CORPORATION - 402 BUSINESS CORPORATION LAW
<b>NFP Category</b>	NO-ANSWER

## Business Entity Information

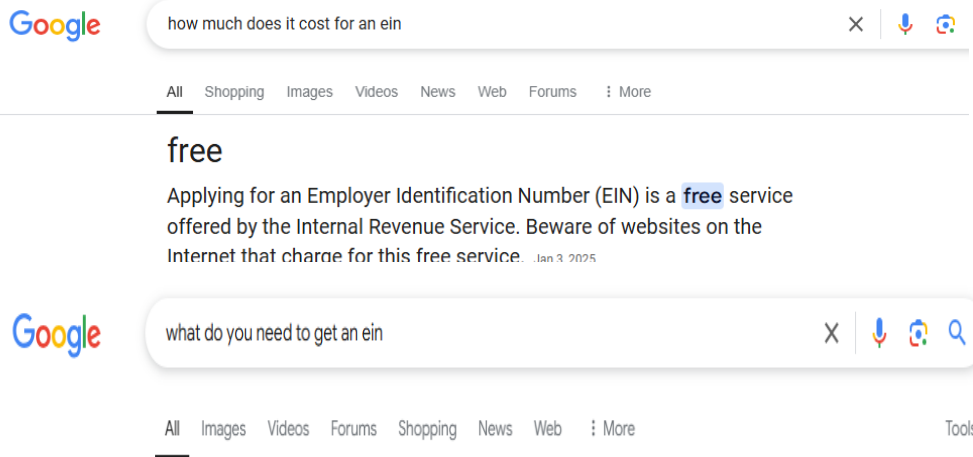
<b>DOS ID</b>	6621450
<b>Current Entity Name</b>	THE BAZOOKA COMPANIES 0 INC.
<b>County</b>	Bronx
<b>Jurisdiction</b>	New York
<b>Entity Type</b>	DOMESTIC BUSINESS CORPORATION
<b>Initial DOS Filing Date</b>	2022-10-21
<b>DOS Process Name</b>	Kashawn Williams
<b>DOS Process Address</b>	4439 Third Avenue Apt 7E Bronx NY 10457

<b>County</b>	Bronx
<b>Jurisdiction</b>	NY
<b>Filer Name</b>	KASHAWN WILLIAMS
<b>Filer Address</b>	4439 Third Avenue Apt 7e Bronx NY 10457-

## Entity Name History

Filing Date	Entity Name	Filing Number	Type	Status
2022-10-21	THE BAZOOKA COMPANIES 0 INC.	221021003171	Actual	Active

# EIN's are FREE- No Authentication Needed



## Beating KYC Over Messaging App

Criminal 1: I'm ready for payment on corp.

Criminal 2: How much

Criminal 1: He's going to be the proud owner of [Entity Name] since Feb 2018; \$550 includes DBA

Criminal 2: Okay I'll go to the bank in a few

Criminal 1: Do you have a blank EIN doc? Let's have it all ready so there is no question moving forward. I'll even give you a link to the state website so they can Verify everything online.

Criminal 2: Verify what? I typically just make a new one and photoshop the notice date and ein

false and fraudulent pretenses, representations, and promises, and by the concealment of material facts.

Object of the Conspiracy and the Scheme to Defraud

18. It was the purpose and object of the conspiracy and scheme to defraud federally insured financial institutions to negotiate stolen business checks into fraudulent accounts established by Defendants and their uncharged co-conspirators, thus giving Defendants and their uncharged co-conspirators access to funds to which they were not entitled.

Manner and Means

19. The manner and means by which the foregoing object of the conspiracy to commit bank fraud was accomplished included, but was not limited to, the following:

- a. Uncharged co-conspirators stole mail matter which contained legitimate business checks written to and intended to be received by legitimate companies, including, but not limited to, the Business Victims; Defendants then obtained those stolen business checks from uncharged co-conspirators.
- b. Defendants and their uncharged co-conspirators registered sham entities with state government agencies, including, but not limited to, the Iowa Secretary of State; such sham entities had names which were identical or substantially similar to the legitimate businesses who were the intended recipients of the stolen checks.

- c. Defendants and their uncharged co-conspirators applied for and received from the IRS EINs for the sham entities.
- d. Defendants and their uncharged co-conspirators recruited others to open and attempt to open accounts at federally insured financial institutions in the names of the sham entities, supplying the individuals they recruited with the stolen business checks and documentation obtained for the sham entities from state government agencies and the IRS.
- e. Using the registration documents and EINs obtained on behalf of the sham entities, Defendants and their uncharged co-conspirators opened and attempted to open accounts at federally insured financial institutions, including, but not limited to, the Financial Institution Victims, in the names of the sham entities with the intent that those accounts would be used for the deposit of stolen checks; to do so, Defendants and their uncharged co-conspirators made materially false and fraudulent representations to the financial institutions and actively concealed material facts from the financial institutions.
- f. When Defendants and their uncharged co-conspirators opened and attempted to open accounts at federally insured financial institutions for the sham entities, or after said accounts had been opened, Defendants and their uncharged co-conspirators deposited, or attempted to deposit, the stolen business checks into the accounts; the Defendants did so with the intent of giving themselves and their uncharged co-conspirators access to funds to which they were not entitled.

20. Through these manners and means, Defendants and their uncharged co-conspirators attempted to negotiate stolen business checks into fraudulent accounts at federally insured financial institutions which, in total, exceeded \$10 million in value.

FILED

AUG 20 2024

CLERK U.S. DISTRICT COURT  
SOUTHERN DISTRICT OF IOWA

IE UNITED STATES DISTRICT COURT  
THE SOUTHERN DISTRICT OF IOWA

Criminal No. 4:24-cr-108

INDICTMENT

T. 18 U.S.C. § 2  
T. 18 U.S.C. § 982(a)(1)  
T. 18 U.S.C. § 1344(1)  
T. 18 U.S.C. § 1344(2)  
T. 18 U.S.C. § 1349  
T. 18 U.S.C. § 1956(h)  
T. 18 U.S.C. § 1957  
T. 21 U.S.C. § 853(p)  
T. 28 U.S.C. § 2461(c)

AMERICA,  
  
LEE,  
le Keessen,  
  
AS,  
la,  
ang, and  
  
ok,  
S,  
een,  
ALEY,  
e, and Bosh,  
  
NSON,  
or,  
Jr.,  
  
L,  
INTER,  
ROE,  
  
TH,  
PP,  
N, Jr., and

# Synthetic Business Fraud

Count	Date	Defendant	Financial Institution	Description of Execution (or Attempted Execution)	Count	Date	Defendant	Financial Institution	Description of Execution (or Attempted Execution)	
2	6	05/15/2023 to 05/16/2023	E. SMITH	GreenState Credit Union	Opening of business account(s) in the name of the sham entity N.C. and then causing to be deposited into said account(s) a stolen business check (in the amount of \$94,096.95) written to Business Victim N.C.	11	07/20/2023 to 07/21/2023	TAPP	Financial Plus Credit Union	Opening of business account(s) in the name of the sham entity C.G. and then causing to be deposited into said account(s) a stolen business check (in the amount of \$93,574.99) written to Business Victim C.G.
						12	08/10/2023 to 08/17/2023	C. THOMAS	Veridian Credit Union	Opening of business account(s) in the name of the sham entity R.M. and then causing to be deposited into said account(s) a stolen business check (in the amount of \$68,800) written to Business Victim R.M.
Count	Date	Defendant	Institution	Execution (or Attempted Execution)	Count	Date	Defendant	Institution	Execution (or Attempted Execution)	
7	05/16/2023	C. THOMAS	Great Southern Bank	Opening account(s) in the name of the sham entity and then causing to be deposited into said account(s) a stolen business check (in the amount of \$156,017) written to Business Victim C.T.O.S.	9	06/15/2023 to 06/20/2023	C. THOMAS	Collins Community Credit Union	Opening of business account(s) in the name of the sham entity B.O. and then causing to be deposited into said account(s) a stolen business check (in the amount of \$53,277.44) written to Business Victim B.O.	
8	05/25/2023	HAYMON	First Central State Bank	Opening account(s) in the name of the sham entity and presenting for deposit into said account(s) a stolen business check (in the amount of \$479,786.63) written to Business Victim Y.A.	10	07/18/2023 to 07/19/2023	RENFROE	Community Choice Credit Union	Opening of business account(s) in the name of the sham entity W.E. and then causing to be deposited into said account(s) a stolen business check (in the amount of \$287,986.51) written to Business Victim W.E.	

# What is ABA Doing?

## PRESS RELEASE

For Immediate Release | March 19, 2024

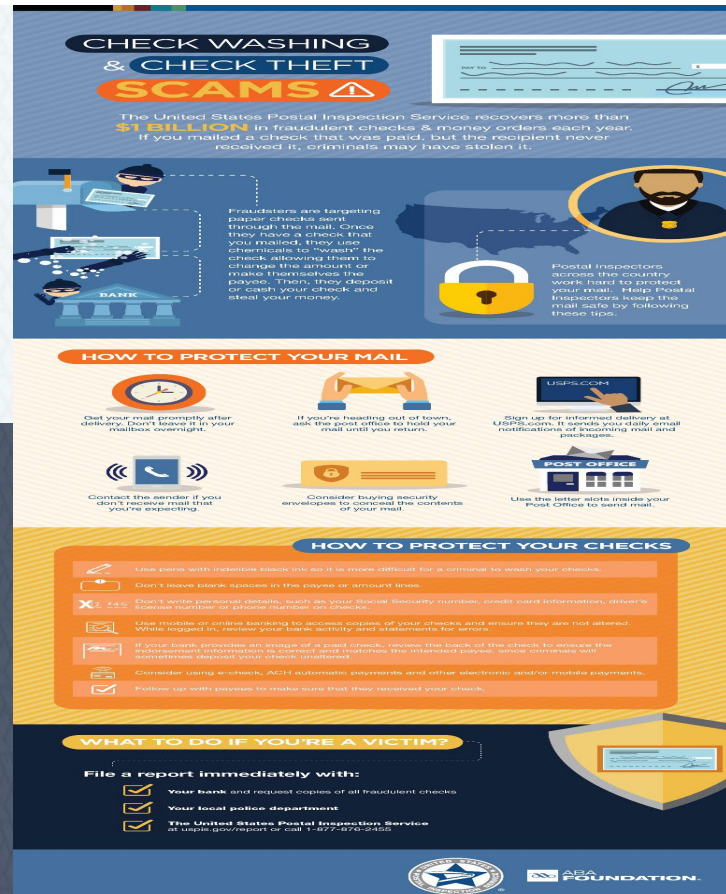
## ABA and U.S. Postal Inspection Service Announce Partnership to Combat Check Fraud

ABA, USPIS release infographic with consumer tips

## WEBINAR

# Mitigating Check Fraud: Tips from USPIS

Aired: February 1, 2024









### CHECK WASHING & CHECK THEFT SCAMS

The United States Postal Inspection Service recovers more than **\$1 BILLION** in fraudulent checks & money orders each year. If you mailed a check that was paid, but the recipient never received it, criminals may have stolen it.







Fraudsters are targeting paper checks sent through the mail. Once they have a check that you mailed, they use chemicals to "wash" the check, allowing them to change the amount or make themselves the payee. Then, they deposit or cash your check and steal your money.

Postal inspectors across the country work hard to protect your mail. Help Postal Inspectors keep the mail safe by following these tips.

#### HOW TO PROTECT YOUR MAIL




-  Get your mail promptly after delivery. Don't leave it in your mailbox overnight.
-  If you're heading out of town, ask the post office to hold your mail until you return.
-  Sign up for informed delivery at USPS.COM. It sends you daily email notifications of incoming mail and packages.
-  Contact the sender if you don't receive mail that you're expecting.
-  Consider buying security envelopes to conceal the contents of your mail.
-  Use the letter slots inside your Post Office to send mail.



#### HOW TO PROTECT YOUR CHECKS

-  Use pens with indelible black ink as it is more difficult for a criminal to wash your checks.
-  Don't leave blank spaces in the payee or amount lines.
-  Don't give out account details, such as your Social Security number, credit card information, driver's license number or phone number.
-  Use mobile or online banking to access copies of your checks and ensure they are not altered. When signed, review your bank activity and statements for errors.
-  If your bank provides an image of a paid check, review the back of the check to ensure the endorsement information is correct and matches the intended payee, since criminals will sometimes deposit your checks online.
-  Consider using e-check, ACH automatic payments and other electronic and/or mobile payments.
-  Follow up with payees to make sure that they received your check.

#### WHAT TO DO IF YOU'RE A VICTIM?

File a report immediately with:

-  Your bank and request copies of all fraudulent checks.
-  Your local police department.
-  The United States Postal Inspection Service at [usps.gov/report](https://usps.gov/report) or call 1-877-876-2465.

# What is ABA Doing?

## Resolve Fraud Claims Efficiently.

The new ABA Fraud Contact Directory helps your bank connect to fraud contacts at other institutions. This searchable database includes bank contacts for ACH, wire, The Clearinghouse RTR, FedNow and check fraud.

ABA member and non-member banks are invited to participate at no cost. The more institutions that get involved, the more helpful the directory will be for the industry.

**Join Today!**

[aba.com/FraudContactDirectory](https://aba.com/FraudContactDirectory)





## Treasury Check Verification System (TCVS)

Issue information for U.S. Treasury checks can be verified provided that the financial institution has a valid routing transit number, check number and check amount. Treasury checks that are older than 13-months old will not be available in this application. These checks should not be cashed by your institution since they are no longer valid after one year. Please inform the payee to contact the issuing agency for additional information.

Please note not all U.S. Treasury checks will contain the unique secure seal. Therefore lack of this seal does not imply the check is a counterfeit.

If no issue record is in the Treasury Check Verification System (TCVS), it does not mean the check is invalid. Please note TCVS was created as a tool to assist in fraud detection, you still need to verify the security features of a U.S. Treasury Check. Also, while not common, a US Treasury Check can be hand signed as opposed to signed by an automated process.

This website is available for use 7 days a week from 6:00am to 12:00am ET.



DEPARTMENT OF THE  
BUREAU OF THE FISCAL  
WASHINGTON, DC 2

### Check

Issue Date

mm/dd/yy

Symbol

nnnn

Serial

nnnnnnnn

Check Amount

\$ 0.00

Bank

RTN

nnnnnnnn

☐ I'm not a robot

Verify



## New payee name validation ability Treasury Check Verification Syst

The Bureau of the Fiscal Service (Fiscal Service) will implement a new payee name validation capability within the Treasury Check Verification System (TCVS) Application Programming Interface (API) on Nov. 18, 2024.

This new feature, which was mentioned in the Federal Reserve System's **March 20, 2024 Notice to Financial Institutions**, helps support Fiscal Service's payment integrity efforts by providing financial institutions with additional data to prevent check fraud.

- **Payee name access will only be available through the API.** The payee name cannot be accessed on the TCVS public website.
- Current API users can retrieve the **new specification document** on the TCVS website.
- To request a key for the API, complete the **Terms & Conditions document** (PDF) on the TCVS website.
- Service providers and financial institutions will not experience any impact to the current TCVS API process and can adapt to the new enhancement at their own pace after Nov. 18.

If you have any questions regarding this new enhancement, please send them to:  
[paymentintegrity@fiscal.treasury.gov](mailto:paymentintegrity@fiscal.treasury.gov).



Banking Topics Training & Events Member Tools News & Research Advocacy About Us



## ABA Fraud Contact Directory

For Bankers Only - Find the right contact to resolve fraud

How to Guides

SEARCH FRAUD DIRECTORY



MANAGE FRAUD CONTACTS



By participating in the ABA Fraud Contact Directory, you agree to the following rules:

- You must provide at least one point of contact for your bank to access the ABA Fraud Contact Directory.
- The contacts in this directory are strictly for use by participating institutions and should NOT be given to customers. Such sharing violates the terms of use and may result in loss of access to the directory.
- You will notify ABA if any contact information is out of date. After ABA communicates receipt of your outdated contact alert, you will have one week to update your contact before it is removed. If all your contacts in the Directory are out of date, your access to the directory will be blocked.

[Read the complete contact directory rules and guidelines to learn the contact's information.](#)

## Fraud Indicator Alerts

Last Updated: 2021-JAN-30 12:00:00

128 Alerts | 97 Shared | 3 Contradicted | 27 Retracted

Link Ref ID	Creditor Agent ID	Creditor ID	Status	Status Up
<a href="#">0097_b886</a>	955708709 ABA	655708709 ACCOUNT NO.	Shared	2020-DE
<a href="#">3165_4985</a>	655708709 ABA	098765434 ACCOUNT NO.	Shared	2020-DE
<a href="#">3265_4985</a>	876545677 ABA	1 FOBS 4345 4548 8274 91 IBAN	Shared	2020-DE
<a href="#">3345_4985</a>	876545677 ABA	notascammer@email.com ZELLE TOKEN	Contradicted	2020-DE
<a href="#">3785_4985</a>	655708709 LEI	1 FOBS 4345 4542 4726 23 IBAN	Shared	2020-DE
<a href="#">3985_4985</a>	876545677 LEI	IBAN UK25 ROJA 2346 4223 8123 98 IBAN	Shared	2020-DE
<a href="#">3125_4985</a>	987654567 LEI	tswiftfan4lyfe@mail.com ZELLE TOKEN	Shared	2020-DE
<a href="#">3235_4985</a>	655708709 LEI	IBAN UK25 ROJA 2346 4205 4294 82 IBAN	Shared	2020-DE
<a href="#">3335_4985</a>	987654567 ABA	1 FOBS 4345 4548 8274 91 IBAN	Retracted	2020-DE

## Alert Details

Shared

SHARED BY

Created by Gemstone Bank  
Created on 2020-DEC-02 08:56:30

### Alert Information

Alert History

CREDITOR AGENT

**Creditor Agent ID** 955708709 ABA  
**First Obsidian**  
Country  
United States

CREDITOR

**Creditor ID** 655708709 ACCOUNT NO.  
Bob's Burgers  
Benito Ocasio

## Current State:

A fraudster can successfully attack victims across various banks, exploiting **delays in account closures** and **gaps in information sharing** across the industry.



## Future State with Data Sharing:

The first bank to identify indicators of fraud **alerts the industry** to help other banks **avert losses for subsequent victims** until the fraudulent account is closed.



# Resources

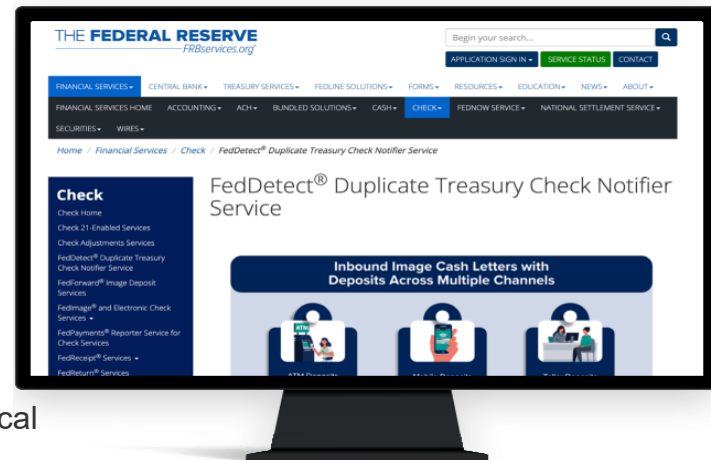
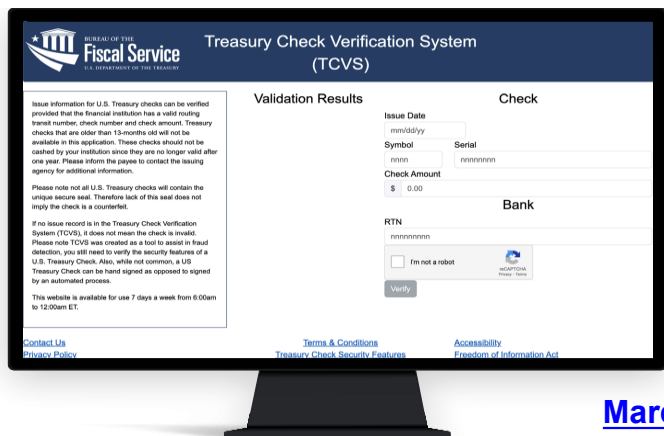
- **Educate**
  - USPIS
    - <https://www.uspis.gov/news/scam-article/check-washing>
  - ABA
    - <https://www.aba.com/news-research/research-analysis/fake-check-scams-infographic>
  - Be timely and creative with educational material to customers and employees
- **Information Share**
  - USSS cyber-fraud center or local cyber-fraud task force
    - <https://www.secretservice.gov/investigation/cyber>
  - 314b Safe Harbor Bank-2-Bank Sharing
  - Vendor information sharing solutions
- **Report**
  - FinCEN – Suspicious Activity Reporting
  - FBI IC3 <https://complaint.ic3.gov/>
  - Postal Inspection Service Victim Reporting
    - <https://www.uspis.gov/report>

# ABA Information Sharing Groups

<u>PROGRAM</u>	<u>Meeting Cadence</u>	<u>Description</u>
National Best Practices	2nd Wednesday, Monthly	This group meets monthly by conference call to examine external fraud with a primary focus on deposit, check, and current overall fraud trends. The participants discuss account fraud prevention systems and techniques used to mitigate risk by the participating banks.
Card Information & Debit Reg E Claims Sharing Group	1st Friday, Monthly	This group focuses on sharing trends and emerging patterns related to credit/debit card authorization, fraudulent transactions, and managing debit issues related to Reg E.
Internal Fraud	4th Wednesday, Bi-Monthly	The Internal Fraud Discussion Group facilitates the sharing of information concerning fraud monitoring and tools, along with fraud trends and investigation results (lessons learned) on topics such as embezzlement, misuse of position and mysterious disappearances by bank employees.

- **ABA Fraud Contact Directory** (ABA.COM)
  - [Fraud Contacts Homepage](#)
- **ABA Initiative: #BanksNeverAskThat and Practice Safe Checks** Campaigns
  - Oct 1, ABA and banks across the country launched a Phishing awareness 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)
- **ABA Check Fraud Toolkit**
  - [2024-check-fraud-toolkit-guide.pdf](#)
- **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>

# Government Tools to Detect Check Fraud



**March 2024, Notice to FIs**, supports Fiscal Service's payment integrity efforts by providing FIs with additional data to prevent check fraud.

- **Payee name access will only be available through the API**, cannot be accessed on the TCVS public website.
- Current API users can retrieve the **[new specification document](#)** on the TC VS website.

## **Postal Money Orders**

<https://tools.usps.com/money-orders.htm>

# ABA & USPIS Partnership

## MONEY MULES

Money mules are the people who transfer money from victims to fraudsters.

Criminals often recruit people through: online job ads, social media platforms, enticing investment opportunities, prize offers or dating websites.

There are three types of money mules. People who are:

- 1 **UNWITTING** — unaware that they are part of a larger scheme.
- 2 **WITTING** — willfully ignore obvious red flags.
- 3 **COMPLICIT** — are aware of their role and actively participate in criminal activity.



### HOW CAN YOU SPOT A MONEY MULE?

Pay attention to the customer's account — both incoming and outgoing funds. Ask yourself these questions:

- Is a customer receiving funds from different people or accounts, and then sending all or most of that money to one account/person or third parties?
- Is there a sudden spike in the customer's deposits or withdrawals?
- Is the customer using transfer methods they have not traditionally used?
- Is the customer receiving funds that the customer can't explain?
- Is the customer's incoming or outgoing payment activity coming from, or going to, high-risk money laundering jurisdictions?
- Are funds coming in from a cryptocurrency exchange and then withdrawn via ATM in international or high-risk jurisdictions very soon after deposit?
- Is the velocity of money transfers unusual?
- Are multiple devices accessing the same account, or is one device accessing multiple seemingly unrelated accounts?
- Has the customer added a new unrelated phone number, email address or physical address to the account?
- Is the account using multiple peer-to-peer platforms in a short period of time?
- Is the same device accessing multiple accounts across the financial institution?

### WHAT NEXT STEPS CAN YOU TAKE?

- Follow your bank's fraud and money laundering procedures.
- Contemporaneously monitor both incoming and outgoing transactions.
- Look for subtle changes in customer behavior.
- Review ANI (automatic number identification) to identify additional accounts that are suspected of fraud, and file collectively (to minimize the number of SAR filings).
- Escalate the issue at your bank for enhanced account monitoring.
- Warn the customer.
- Notify law enforcement.

If you witness crimes targeting the U.S. Mail or Postal employees, call the police, then call Postal Inspectors at 1-877-876-2455.

Report all suspected mail theft to the United States Postal Inspection Service at [uspis.gov/report](https://www.uspis.gov/report).

Also, report it to the Federal Bureau of Investigation at [FBI.gov](https://www.fbi.gov).



## MONEY MULES

If someone sends you money and asks you to send it to someone else, **STOP.**

YOU COULD BE A MONEY MULE

someone who criminals use to transfer and launder illegally acquired money. Criminals might try to recruit you through online job ads, social media, enticing investment opportunities, prize offers or dating websites.

If you participate in the scam, you could lose a lot of money or end up with an overdrawn account. You could also get into legal trouble as an accomplice to a crime.

### HOW TO AVOID A MONEY MULE SCAM

- ✓ Do not use your own bank account, or open one in your name, to receive or transfer money for an employer or for anyone else.
- ✓ Do not accept or endorse a check that's not in your name, even if a friend or employer asks you to do it.
- ✓ Do not incorporate a fictitious business to deposit a check corresponding to a similarly named business.
- ✓ Never pay to collect a prize or transfer money from your "winnings."
- ✓ Never send money to online love interests, even if they appear to send you money first.
- ✓ Do not listen to anyone offering you a great cryptocurrency investment or asking you to deposit money into a Bitcoin ATM.
- ✓ Never purchase cryptocurrency or gift cards on behalf of, or for, someone you met online or over the phone.
- ✓ Never share your bank passcodes, including one-time verification codes, or provide anyone with access to your bank account, online credentials, debit card number or PIN.
- ✓ Always monitor your accounts and report suspicious activity to your bank.

### WHAT TO DO IF YOU SPOT THE SCAM



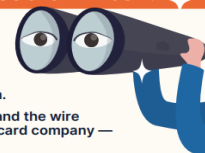
End all contact with the criminals and stop moving money for them.



Tell your bank and the wire transfer or gift card company — right away!



Report it to the Federal Bureau of Investigation at [FBI.gov](https://www.fbi.gov) and the United States Postal Inspection Service at [uspis.gov/report](https://www.uspis.gov/report).



Criminals are good at tricking people into helping them move money. **DON'T DO IT.** You could lose your money and get in trouble with the law.

