Statement for the Record

On Behalf of the

American Bankers Association

Before the

Government Operations Subcommittee

Of the

House Committee on Oversight and Government Reform

July 23, 2025

Statement for the Record

On Behalf of the

American Bankers Association

before the

Government Operations Subcommittee

Of the

House Committee on Oversight and Government Reform

July 23, 2025

The American Bankers Association (ABA) appreciates the opportunity to provide a Statement for the Record for this hearing entitled, "An Update on Mail Theft and Crime." ABA is the voice of the nation's $24.1 trillion banking industry, which is composed of small, regional, and large banks that together employ more than 2.1 million people, safeguard $19.2 trillion in deposits and extend $12.7 trillion in loans.

Background on Mail Theft and Crime

Check fraud has increased over 385% nationwide since the onset of the COVID-19 pandemic.[1] In response, the ABA and member banks have made combating this rapidly growing threat a top priority, as criminal organizations increasingly rely on check fraud to perpetrate financial crimes.

Check fraud schemes commonly begin with a theft of a check from the U.S. mail system, leading to check alterations and counterfeit checks created from the image of the stolen check. Criminals then move quickly from the point of theft to depositing the compromised check(s) into a bank account to steal money.

These schemes range from the simple - a street-level complicit actor taking an altered/washed check to a bank branch to deposit, to the complex - like a counterfeit check image being deposited into a criminal controlled account using remote deposit channels. Even using the oldest, most transparent monetary instrument in America (a check), the criminals can leverage the two most difficult factors to defend against bank related frauds today, speed and anonymity.

ABA and the U.S. Postal Inspection Service (USPIS) quickly recognized the need for cross-industry collaboration to combat the growing wave of organized check fraud. In March 2024, the ABA and USPIS publicly announced a formal agreement to launch a joint Fraud Awareness Campaign. The joint initiative focuses on four main areas:

[1] https://home.treasury.gov/news/press-releases/jy2134

- Educating U.S. Postal Service and bank customers about check fraud and what they can do to protect themselves
- Addressing money mules and collusive accountholders
- Collaborating with law enforcement
- Training bank employees and postal workers on red flags and prevention.

ABA – U.S. Postal Inspection Service Joint Fraud Awareness Campaign

Through the partnership, we have placed a strong emphasis on training banks. ABA featured USPIS as a keynote speaker at its Check Fraud Symposium, which included banks of all sizes, industry vendors, and key government agencies. USPIS has also served as a valuable resource on approximately five ABA webinars and podcasts, enabling us to reach banks across the nation. These speaking engagements have provided banks with critical insights into the importance of robust information sharing with USPIS, particularly in navigating a challenging prosecutorial landscape. As a result, banks have a clear understanding that check fraud investigations are a priority—and that the speed and thoroughness of their reporting significantly enhances the effectiveness of these investigations.

Building on the need for public-private information sharing, USPIS also regularly engages with banks and ABA on check fraud in monthly ABA working group meetings. Through these meetings, bankers learn about evolving criminal trends, regional crime patterns, red flags associated with new fraud techniques, and guidance on where to report suspicious activity—including key elements that should be included in those reports. USPIS has also briefed bankers on the joint USPIS and FinCEN initiative to better track check fraud activity in a timely manner. Banks now report to FinCEN using a key term when filing a suspicious activity report (SAR) to ensure that USPIS receives information about suspected check fraud activity.

ABA and USPIS have also presented together at law enforcement and private industry conferences and meetings, such as the International Association of Financial Crimes Investigators (IAFCI) and Financial Industry Mail Security Initiative (FIMSI) sponsored events. These events are well attended by local police departments looking for training and information relating to check fraud in their communities.

Joint training sessions provide substantial benefits to both banks and law enforcement agencies, fostering stronger collaboration in the fight against criminal activity. These sessions help clarify emerging criminal tactics that target both consumers and financial institutions alike. For instance, a growing threat involving the rapid movement of stolen checks and check images across state lines—from California to New York—via encrypted platforms like Telegram, poses significant challenges for prosecution given cross-jurisdictional activity. Through joint training, participants share best practices on how to identify, preserve, and report critical evidence.

In addition to the partnership, ABA offers tools to banks and others that help in this fight against check fraud, such as the ABA Fraud Contact Directory and the ABA Treasury Check Payee Verification System ABA hosted application programming interface (API) connection, to name a few. The Fraud Contact Directory houses fraud contacts of participating banks for check fraud processing and all other payment types. Most recently, ABA also teamed up with the Treasury

Department to create a centralized point of entry for banks to the Treasury Check Verification System's (TCVS). The Treasury Department offers a direct connection, via an API, to validate Treasury Checks and their payees to all financial institutions. ABA now hosts the API for banks to access the TCVS with payee verification quickly, with no additional setup steps. Thousands of bank inquiries have been made to the Treasury from this ABA hosted platform since the launch date, June 12, 2025.

Public Education – Infographics

In recognition of the growing need to educate the public on check fraud and related criminal tactics, ABA and USPIS developed a series of four infographics[2] as part of our ongoing efforts to safeguard Americans from financial scams. Each infographic is tailored to a specific audience and provides targeted, practical guidance:

- **Consumers** – Check Washing Prevention: To help individuals protect against check washing, the resource advises:
    - Using pens with indelible black ink to make alterations more difficult;
    - Avoiding blank spaces in the payee and amount lines;
    - Refraining from writing sensitive information (e.g., Social Security numbers, credit card details, or driver's license numbers) on checks;
    - Following up with payees to confirm receipt of checks.
- **Small Business Owners** – Check Fraud Prevention Measures: Small business owners are encouraged to:
    - Implement a "need-to-know" policy to restrict employee access to sensitive information and business checks;
    - Consult with financial institutions about fraud monitoring services and prevention tools;
    - Utilize positive pay services to validate issued checks and prevent unauthorized payments; and
    - Verify that all financial instruments issued from business accounts are received by the intended recipients.
- **Consumers** – Avoiding Money Mule Scams: To reduce the risk of being exploited in money mule schemes, the infographic advises individuals to:
    - Avoid using personal bank accounts or opening new accounts to receive or transfer funds on behalf of third parties;

[2] See appendix at end of document for infographics

- Refrain from sharing banking credentials, one-time passcodes, debit card numbers, PINs, or granting access to online banking platforms;
- Decline to accept or endorse checks not issued in their name;
- Avoid forming fictitious businesses for the purpose of depositing checks payable to similarly named entities.

- **Banks** – Detecting Money Mule Activity:
  - Aimed at financial institutions, this infographic outlines best practices for identifying potential money mule activity. It emphasizes the importance of monitoring both incoming and outgoing transactions and highlights key red flags to spot unusual account activity.

ABA National Consumer Campaign

In addition to joint efforts with USPIS, the ABA launched a national consumer campaign in October 2024, titled "#PracticeSafeChecks," which coincided with ABA's ongoing "#Banks NeverAskThat" anti—phishing campaign. Partnering with more than 1,600 banks across the country, the campaign is intended to help consumers protect themselves against check fraud and encourages the use of secure digital banking tools for sending money.

The campaign features educational videos that use humor to engage consumers while delivering clear, actionable fraud prevention tips. ABA and our member banks are sharing these resources—including videos, striking graphics, and safety tips—across social media platforms, websites, ATM screens, and bank branches nationwide.

ABA provides all campaign materials free of charge to member and non-member banks, allowing participating institutions to customize and deploy the content in ways that best serve their local communities, while consumers can visit https://practicesafechecks.com.

Conclusion

Industry innovation provides more payments options for consumers and small businesses every day, but for the moment, many Americans still want to use checks. Until consumers and businesses recognize the clear benefits of using safer digital options, criminals will continue to exploit the inherent flaws in paper checks. To successfully fight back will require greater collaboration and cooperation between federal, state, and local agencies alongside private sector stakeholders such as America's banks. We have specifically urged the administration to consider creating an office in the White House to develop a coordinated national strategy for combatting fraud, including check fraud.

Until then, ABA will continue working with as many stakeholders as possible to respond to the fraud challenge. ABA appreciates the close collaboration with the USPIS to date, and we look forward to continued opportunities to advance our shared goal of protecting consumers from check fraud. Thank you once again for allowing us to provide our views on mail theft and crime.

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 so it is more difficult for a criminal to wash your checks.
- Don't leave blank spaces in the payee or amount lines.
- Don't write personal details, such as your Social Security number, credit card information, driver's license number or phone number on checks.
- Use mobile or online banking to access copies of your checks and ensure they are not altered. While logged in, 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 indorsement information is correct and matches the intended payee, since criminals will sometimes deposit your check unaltered.
- 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 uspis.gov/report or call 1-877-876-2455

UNITED STATES POSTAL INSPECTION SERVICE®

ABA FOUNDATION®

Protect Your Business from

CHECK FRAUD

Has your business had checks stolen or altered? Have your accounts been subject to counterfeit checks or unauthorized withdrawals? If you answered yes to either of these questions, your business could be the target of a check fraud scheme.

Bad actors target business financial accounts over personal accounts because of large transaction volumes, more funds, and higher liquidity, making it easier to cash higher dollar counterfeit or altered checks — and more difficult to detect fraudulent transactions and overdraft issues. Securing your checks is vital!

BAD ACTORS COULD:

- Target business accounts by intercepting outbound or inbound mail.
- Recruit "insiders" to gain access to sensitive information such as bank account numbers or personally identifiable information (PII).
- Obtain examples of legitimate monetary instruments, such as business or cashier checks, in order to duplicate the banking details onto counterfeit checks.
- Purchase account details and business checks through an online forum.

HOW TO PROTECT YOUR BUSINESS:

- Adopt an employee need-to-know policy to limit access to sensitive information and business checks.
- Talk to your bank about services to monitor business account activity, such as fraud prevention programs (FPPs). FPPs can require and request verification for all checks drawn against specific accounts to detect and prevent fraudulent activity.
- Explore the use of a Positive Pay product with your bank to add another layer of validation protection to the check process.
- Confirm that all financial instruments drawn from your business accounts are received by the intended recipients. Any outstanding items should be flagged.
- Use the letter slots inside your post office for your outgoing mail or hand it directly to a letter carrier. Pick up your mail promptly after delivery. Don't leave it in your mailbox overnight. If you do not have weekend hours, coordinate with your local post office to hold any weekend mail until the following business day.

WHAT TO DO IF YOU SPOT THE SCAM:

- Report the fraud to your bank right away! If feasible, change your account number(s). Bad actors often reuse account details and/or sell them online, resulting in additional counterfeit attempts and fraudulent activity.
- Report it to your local police department immediately and report all suspected mail theft to the United States Postal Inspection Service at uspis.gov/report or at 1-877-876-2455.

UNITED STATES POSTAL INSPECTION SERVICE®

ABA FOUNDATION®

MONEY MULES

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

STOP.

YOU COULD BE A MONEY MULE

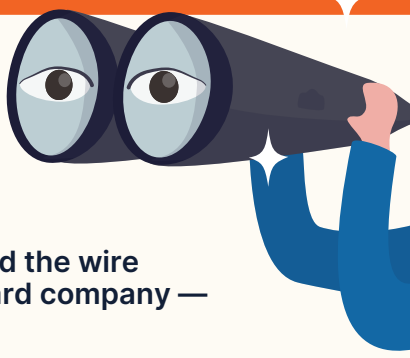
someone who criminals use to transfer and launder illegally acquired money. Criminals might try to recruit you through online job ads, social media, enticing investment opportunities, prize offers or dating websites.

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 **IC3.gov** and the United States Postal Inspection Service at **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.

UNITED STATES POSTAL INSPECTION SERVICE®

ABA FOUNDATION®

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**.

Also, report it to the Federal Bureau of Investigation at **IC3.gov**.

UNITED STATES POSTAL INSPECTION SERVICE®

ABA FOUNDATION®