Testimony of

Gay G. Dempsey

Chief Executive Officer
Bank of Lincoln County
Fayetteville, Tennessee

On behalf of the

Independent Community Bankers of America

Before the

U.S. House of Representatives
Committee on Financial Services
Subcommittee on Financial Institutions

Hearing on

"Fighting Fraud on the Front Lines:
Challenges and Opportunities for Financial Institutions"

March 5, 2026
Washington, D.C.

Chairman Barr, Ranking Member Foster, and members of the Subcommittee, I am Gay G. Dempsey, CEO of the Bank of Lincoln County in Fayetteville, Tennessee.

I am a member of the Board of Directors of the Independent Community Bankers of America, or ICBA, where I am also the Tennessee Federal Delegate and am active on several committees, including the Fraud and Scams Task Force. I am also active in the Tennessee Bankers Association where I am Vice Chairman of the Board and soon-to-be Chairman. I testify today on behalf of ICBA and thousands of community banks across the country.

Thank you for convening today's hearing on "Fighting Fraud on the Front Lines: Challenges and Opportunities for Financial Institutions."

Escalating fraud losses are a priority concern for community banks. A lifelong community banker, in recent years I have dedicated considerable time and effort to fighting payments fraud and scams, having witnessed at first hand the impact on my customers, my bank and peer community banks, local small businesses, and our community. Fraud creates financial ruin for too many individuals and endangers local prosperity.

At my bank, fraud losses—originating outside my bank—exceed loan losses, despite our best efforts at prevention and significant anti-fraud investments. Sadly, this has been true for the last 10 years and is true of many other community banks today. As important as loan underwriting and asset management are to a bank's success, in today's environment, fraud management takes precedence.

The problem is urgent and must be fought through coordination among financial institutions of all charter types and sizes, law enforcement, and government at every level. This hearing and the work of this committee are very much a part of that effort. My statement contains legislative and regulatory recommendations, but I ask you to understand that any additional mandates on community banks would be counterproductive. More regulation on an already-burdened industry is not an effective solution.

Before I go any further, I would like to thank Chairman Hill, Chairman Meuser, Rep. Foster, and the many members of this committee, for your letter of November 2024 to the financial agency heads clarifying the scope of the check-fraud problem and emphasizing the need for a coordinated, cross-agency response to better allow financial institutions to protect American consumers and businesses.

Our Story

The Bank of Lincoln County is a $225 million asset bank with three branches and 44 employees. Lincoln County has a population of 35,319 and borders Alabama in Southern Middle Tennessee. My community of Fayetteville has a population of approximately 8,000.

We were founded in 2002, by my family and several other local business leaders, when we recognized

the need for a locally owned bank to create an economically stabilizing influence in Lincoln County. The sale of a local bank, in which I began as a teller in high school and rose into leadership, had left a gap in banking services with harmful impact. Recognizing this, we founded a new bank, which has thrived in lending to local families, small businesses, and farmers. Thousands of community banks around the country, many of them family-owned, were founded on that same vision. When any member of our small community falls victim to fraud, it hurts the whole community.

Fraud in my Bank and my Community

I would like to share with you a few stories to illustrate the impact of fraud in Lincoln County, Tennessee.

Stolen checks: Better interbank resolution and the involvement of the Fed is critical to funds recovery

In 2022, a small business customer of ours had 15-20 checks totaling almost $600,000 stolen from the mail, and the payee was altered. The vast majority of these checks were mobile deposited at several larger banks.

As soon as the alterations were discovered, Bank of Lincoln County gave our customer immediate credit for the checks and began the arduous process of recovering the funds.

The window for returning checks is midnight of the next banking day. This would have been the easiest way to recover the funds.

However, the business maintains high balances at BOLC and understandably did not notice the posting of stolen checks until the window had closed. The first line of defense, the short return window, is simply impractical for many small businesses and consumers, who should not be expected to constantly monitor their accounts.

With that option closed, we returned the checks through the Federal Reserve claiming “Breach of Warranty.” Accepting deposit of an altered check is a clear breach of warranty. Such claims are exempt from the midnight return deadline.

With the mediation of the Fed, we pursued our case under UCC law and eventually recovered 100 percent of the funds. However, the recovery process took almost six months, and that delay is a hardship to a small community bank. It makes it more difficult for us to serve our community.

The Fed’s role in mediation was critical to the recovery. In 2023, all such matters were mediated by the Federal Reserve, and the Federal Reserve would enforce “timeliness in correspondence,” ensuring that each party is responsive to the other, from the initial claim until the matter is resolved.

Unfortunately, the Fed no longer enforces timeliness of correspondence. A payor bank, BOLC in this case, makes an initial return through the Fed, and if it is denied, the bank must pursue its claim directly with the bank of first deposit, which is not held to a timeliness standard and may not respond at all. The Fed has removed itself from the process after the initial return and response, and larger banks have no incentive to be responsive.

Today, it is doubtful that we would have been able to recover the funds. *This is exactly why we need a more effective interbank dispute resolution process, as I discuss later in this testimony.*

Too often, recovery is not possible

Also in 2023, a BOLC cashier's check for $118,000 was stolen in the mail, altered, and deposited at a large bank. The depositor was a fake business, an LLC created in Georgia expressly for the purpose of perpetuating a fraud.

We discovered the alteration within five days; however, the fraudster had promptly withdrawn the majority of the funds.

Again, we pursued a "breach of warranty" claim—the depositing bank should not have accepted the deposit. The depositing bank claimed that the check was "counterfeit," which would put the liability on my bank. I maintain that the check was "altered," which puts the liability on the depositing bank.

For eight months we tried to make contact with the large bank to respond to our breach of warranty claim. We wrote letters and called every number we could find. I finally found a contact with the help of the Tennessee Bankers Association. That person responded to our first email and then went silent. It was beyond frustrating.

We hired a lawyer since it was, to us, such a large amount.

We eventually lost that case because the large bank's "expert" testified that the check was counterfeit under the current definition. Borders and minute security language had been digitally altered, details you would not catch without a microscope. The check number, amount, date, bank logo, address, signature and other characteristics were all the same. Only the payee had been changed.

When all was said and done, BOLC lost $118,000 plus lawyer's fees.

What's more, I later learned that the fraudulent account had $11,000, which the large bank had withheld from us. After three requests and more than a year, the bank finally returned the $11,000 to our bank. Transparency was lacking.

Both of these cases of check theft and alteration could have been prevented with better mail security and better KYC at the depositing bank. The accounts should never have been opened, and the deposits should never have been accepted. Further, the state of Georgia should not have continued to open LLCs for an individual with so many red flags.

The UCC Permanent Editorial Board should revisit and modernize the definitions of counterfeit and altered, which were written before today's digital alteration techniques existed. Interbank disputes and liability depend on these outdated definitions.

There are many points of vulnerability in our system.

Imposter scams exploit weak social media standards

In addition to check fraud, numerous customers have also been victimized by imposters who used social media to trick, deceive, or gain the trust of their victims.

The most heartbreaking case was an elderly woman with no family who fell victim to a romance scam perpetrated through social media. A man convinced her to sell her house for $85,000, and the proceeds were deposited at BOLC. Recognizing the likely scam, we refused her request to wire the money to the scammer and tried everything we could to convince her that she was a victim, including showing her FBI reports, but she didn't want to believe it. Romance scams are just that powerful.

She visited a branch to make a cash withdrawal. Though we could not refuse the request, we asked her to sign a form indicating that we advised her not to carry that much cash with her.

Rejecting our advice, she took the cash and went straight to a local convenience store with a Bitcoin ATM, deposited the money and transferred it to the scammer. As predicted, he was never heard from again. Today, she lives in subsidized housing. I have to believe that this fraud could not have been perpetrated without the use of fake social media accounts. It was a preventable crime.

Manipulative tactics continue to evolve and create more victims

A few more stories will illustrate how manipulative, coercive, and destructively creative fraudsters can be.

More than once, a customer has walked into a branch with a scammer on their cell phone directing them to wire money or withdraw cash based on outlandish premises. They may have been led to believe that they owed the government money and might be arrested or that they had been mistakenly overpaid by a company (for example, $40,000 instead of $400) and faced demands to promptly refund the excess. One case began when a customer clicked on a fake anti-virus warning and was led down a rabbit hole of deceit believing that she owed money.

My tellers do a great job of identifying and escalating these cases to me, and we always tell the customer: Just hang up the phone! Sometimes that's the end of it, but not always.

In one case we worked with a victim and the local sheriff to create a sting operation for the fraudster who, not satisfied with a first payment of $30,000, insisted on an additional payment of $10,000. By this time the victim had realized her mistake and contacted our bank. We worked with local law enforcement who laid a trap for the fraudster. I'm proud of the role our bank played in this case, which led to an arrest but, unfortunately, not the recovery of the victim's money.

These are just a few examples that illustrate different types of fraud and different vulnerabilities of American consumers, small businesses, and community banks. I've seen so many victims, some of whom I could help and some not. The hundreds of community bankers from across the country I've met all have similar stories. We need help to stem the rising tide of fraud. We need to work together, across industries, and with government at every level to strengthen the weak links in the system.

The Impact of Fraud

The scope and impact of fraud and scams have been on a steep upward trend at least since the pandemic, impacting more families, small businesses, and community banks than ever before. National polling conducted by ICBA and Morning Consult found that one in five consumers have been—or know someone who has been—a victim of check fraud.

While there is no single data source that comprehensively captures this trend using consistent definitions and collection methods, the available data tells a consistent and disturbing story. The FBI's Internet Crime Complaint Center (IC3) collects reports of consumer and business cybercrime and elder fraud. The most recent report of IC3, from 2024 and limited to certain types of fraud, indicates losses of $16.6 billion, an increase of 33 percent over the prior year. There were over 256,000 complaints with actual losses with an average loss of $19,372. People over 60 years of age reported, by a wide margin, the largest losses of any age group, $4.8 billion in total. The largest categories of scams were investment scams (over $6.5 billion in losses), business email compromise (over $2.7 billion), and technical support scams (over $1.4 billion).

The FTC's Consumer Sentinel Network Data Book reports fraud losses in 2024 of $12.8 billion, with a median consumer loss of $499. The median loss is much higher among victims aged 70 to 79 ($1,000) and aged 80 and above ($1,650). Imposter scams accounted for almost $3 billion in losses with a median loss of $800. The FTC reports an increase in losses in 2024 over the prior year of 25 percent.

The Global Anti-Scam Alliance's report, "The State of Scams in the United States—2025," finds that the average American encountered a scam attempt 377 times per year. According to that report, the most common payment methods used in scams are debit cards (30 percent of cases) and PayPal (25 percent of

cases).

FinCEN reports that SARS related to mail theft check fraud were associated with $688 million in transactions over a period of just six months in 2023. FinCEN's Year in Review has 4.7 million total SARs filed in FY 2024, averaging 12,870 a day. The Federal Reserve's Consumer Compliance Outlook reported a 110 percent increase in fraud-related SARs from 2020 to 2024 (552,920 to 1,165,642).

All available data indicate that fraud is a social and economic reality that must be confronted with urgency by policymakers in conjunction with financial institutions and law enforcement.

Community Bank Impact of Fraud

How does fraud affect community banks? First, as should be obvious, fraud losses disproportionately impact community banks relative to our asset sizes. A large bank with hundreds of billions or more than a trillion dollars in assets can more easily absorb fraud losses. For a bank like ours, fraud losses make a fundamental impact on our ability to serve our local community. Again, these are losses that originate outside our bank and beyond our control, but for which our bank is liable.

Beyond the significant dollar losses, fraud is increasingly absorbing my time, focus and attention as CEO, and that of every member of my staff. Time spent fighting fraud steals valuable time we should all be spending taking care of our customers and our communities.

The intangible impact of fraud is also significant. I refer to the inevitable erosion of customer trust in my bank and all financial institutions. When a fraudster impersonates a bank by phone, text or email or steals a check, consumers understandably lose trust in all banks and, ironically, seek out unregulated, non-bank alternatives that put them at even greater risk.

For a community bank, relationships are our stock-in-trade and our competitive advantage over larger, transaction-oriented banks. Fraud jeopardizes these critical relationships, and that's why we are so committed to fighting it.

ICBA and Community Bank Response

Given the high stakes I have described, how are community banks responding to the challenge of fraud?

Technology and Training

First, community banks are investing significant amounts in technology to detect fraud. A few tools that our bank has implemented are Positive Pay with Payee Matching, which is deployed through our core processor. Our bank also utilizes several reports and services offered through the Federal Reserve. We have also contracted with a vendor using AI to build a repository of scanned checks. This system

attempts to identify twenty data points on a check and to "learn" those points. Each time a check is presented it is scanned to verify those points and authenticate the check. While this system has caught several fraudulent checks, it has also missed several because the digital alterations appear authentic. Each of these tools add significant costs for our bank.

Second, to leverage our technological investments and to get the most value from them, we invest significantly in training our staff to spot indications of fraud, such as unusual account activity, and to report suspicious activity. Staff, whether they are in the lobby, answering the phone, or in the back office, are the point of customer contact and positioned to detect fraud early and intervene. Their training is critical but so are the personal relationships they have formed with customers. Advice is taken more seriously coming from a banker you've known for years, from clubs, PTA, sports or other activities. As members of a close community, we look out for each other. Again, these relationships are the community bank advantage, and our team does an incredible job of identifying fraud on the front line.

Industry Coordination and Information Sharing

Fraud and Scams Task Force. Several years ago, ICBA created a fraud task force, on which I serve, that brings together community banks and state associations from across the country to share information and best practices, build relationships with regulators, and collaboratively develop resources for our peers. Notably, ICBA and the task force have jointly released a series of resources that address check fraud, including a comprehensive guide to liability, a survey of detection mechanisms, and instructions for how to escalate interbank disputes to regulators.

Acting in Partnership with the U.S. Postal Inspection Service

By far the biggest source of stolen checks is the United States Postal Service (USPS). Checks are stolen from consumer mailboxes as well as from USPS facilities. USPS became a rich source of checks for criminals, particularly government benefit checks distributed through the mail. Effective mail security is a critical, though not exclusive, part of the solution to the problem of check fraud. With better security, check fraud would be significantly reduced.

ICBA partnered with the US Postal Inspection Service to produce an in-branch handout for community bankers to share with customers and start a conversation about fraud and scams prevention. Hundreds of thousands of copies have been distributed to hundreds of banks across the country. We believe this is a model for targeted partnership with a government agency to produce tools and resources to help community banks combat fraud and scams.

Educating Community Banks and their Customers

ICBA's Fraud Task Force has released a series of resources that address check fraud, including a comprehensive guide to liability, a survey of detection mechanisms, and instructions for how to escalate interbank disputes to regulators. Our Task Force is an invaluable forum for sharing best practices among community banks.

ICBA delivers a broad range of educational content to help banks develop and implement their strategies to combat fraud and scams, including comprehensive coursework and topical webinars.

Broad Based Stakeholder Efforts

Collaborative stakeholder efforts play an important role in addressing payments fraud. Fraud and scams persist across state borders and involve stakeholders across economic sectors. National collaboration, including collaboration across federal agencies outside of the banking sector, is necessary to effectively combat the problem.

Support for Recent Administration Initiatives

ICBA is pleased to see the beginning of a coordinated federal effort to address the persistent threat of fraud and scams:

- **Executive order and request for information on phasing out paper Treasury checks.** In March 2025, the administration issued an executive order ordering the federal government to stop using paper checks for disbursements and receipts. In June 2025, the U.S. Department of the Treasury issued a request for information on the executive order. ICBA supports the administration's effort to combat the threat of check fraud[1] and submitted a comment letter in response to the request for information.[2]

- **Request for information on payments fraud.** In June 2025, the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, and Federal Deposit Insurance Corporation issued a request for information seeking input on actions the agencies could take to help mitigate payments fraud. The request for information covered five potential areas for improvement and collaboration that could help mitigate payments fraud. ICBA submitted a comment letter, alongside a letter cosigned by its affiliated state and regional affiliates and many letters prepared by individual community banks. Some of our recommendations from that letter are discussed below.

---

[1] https://www.icba.org/newsroom/news-and-articles/2025/03/26/icba-applauds-trump-administration-on-executive-order-combating-check-fraud

[2] https://www.icba.org/docs/default-source/icba/advocacy-documents/letters-to-regulators/icba-response-to-modernizing-payments-executive-order-rfi-1-(1).pdf

ICBA looks forward to continuing to work closely with the administration and regulators to help community banks combat fraud and scams.

Changes We Need to More Effectively Fight Fraud

There are opportunities to enhance supervisory guidance around appropriate controls, suitable technology, reporting, and incident response, but it is important to avoid imposing new burdens on community banks. Payments fraud regulations and examiner expectations need to be appropriately tailored to community banks with tiered compliance requirements and deadlines.

Changes to Regulation CC

Hold times

Federal Reserve Regulation CC governs the availability of funds, including hold times, and the collection and return of checks. Changes to Regulation CC could help community banks prevent and mitigate check fraud.

ICBA would not support shortening Regulation CC hold times across the board, as this would limit banks' ability to effectively detect and mitigate check fraud by reducing the amount of time banks have to review checks. However, Regulation CC should allow longer hold times for mobile check deposits or under other appropriate circumstances, including, for example, new accounts or accounts that display certain usage patterns. Providing additional flexibility to hold funds would provide significantly greater opportunity to identify suspected payments fraud.

"Reasonable cause to doubt"

Regulation CC allows depository institutions to extend deposit hold periods when the institution has a "reasonable cause to doubt the collectability of a check," among other exceptions. ICBA believes the existing "reasonable cause" standard is vague and creates uncertainty for community banks. While this is a valuable exception, clearer guidance would help increase community banks' confidence in invoking the exception. A safe harbor that would apply when certain conditions are met would also encourage community banks to invoke the exception.

Interbank dispute resolution process

Community banks report that large financial institutions often reject fraud claims even when they provide significant documentation. In addition, contacts are difficult to find (despite the existence of third-party directories), and communication timeframes are often long. As a result, community banks are often forced to absorb losses when they have legitimate claims.

An appropriately tailored resolution process could provide more standardized, timely, and effective resolution of interbank disputes. This would enable community banks to pursue check fraud claims much more efficiently, increasing certainty across the ecosystem.

Liability standards

Regulation CC should explicitly define liability allocation for specific fraud scenarios, particularly for altered checks and forged endorsements. Clear definitions would help level the playing field for community banks and large financial institutions that currently exploit ambiguous rules to shift losses to community banks.

Federal Reserve check services help catch fraud and should not be discontinued

In December 2025, the Federal Reserve Board published an RFI on the future of the Reserve Banks' check collection and processing services. The Reserve Banks offer these services, including multiple daily deposit deadlines, return processing, and discrepancy resolution, to banks and credit unions for a fee. For many community banks, the Reserve Banks are the primary or sole check processing provider. Private sector alternatives are generally designed for larger institutions with greater volume and bargaining power.

I shared a story above about how the Federal Reserve's intervention in a breach of warranty claim helped my bank recover funds in a stolen and altered check case. The Federal Reserve's withdrawal from check services and the valuable role it plays in dispute resolution would only expose community banks to more fraud losses that should rightfully reside with larger banks.

We are pleased that Federal Reserve Vice Chair for Supervision Michelle Bowman recognizes the Fed check services and issued a statement opposing the RFI. We urge this committee, in your oversight of the Federal Reserve, to support continuation of check services.

Bills Before the Committee Today

I thank the committee for posting three draft bills for discussion today. Each of them would be helpful.

The ''Transaction Risk Analytics and Collaborative Exchange (TRACE) Act of 2026''

The TRACE Act would authorize controlled sharing of fraud-related information among financial institutions, protect consumer privacy, and enable artificial intelligence-based detection systems.

This legislation is thoughtfully crafted and would be useful in expanding lawful fraud information sharing and providing safe harbors. These are critical provisions. To further strengthen this legislation, ICBA recommends the following changes:

- Add Explicit Proportionality for Community Banks

We recommend the addition of language to direct regulators to consider institutional size and complexity.

- Clarify "Reasonably Necessary" Scope of Covered Information Definition

The definition of "covered information" is broad, as appropriate. However, the "reasonably necessary" standard could benefit from clarification, in Section 2, to prevent overcollection concerns. We suggest the following language.

Information shared shall be limited to what is reasonably necessary and proportionate to the covered fraud-prevention purpose and consistent with data minimization principles.

This language reinforces privacy protections while preserving flexibility for community banks.

With these additions, the legislation would better reflect the operational realities of community banks while preserving strong privacy and data governance priorities.

The ''Scrutinizing Transactions for Overt Payment Fraud (STOP Fraud) Act of 2026''

This legislation would amend the Expedited Funds Availability Act to provide exceptions in the case of fraudulent checks or wire transfers.

ICBA supports this legislation. As discussed above, longer hold times are appropriate in certain cases and will allow community banks to stop more fraudulent transactions.

The "Bank Fraud Technology Advancement Act of 2026"

This legislation would require the Federal banking agencies to conduct a study on the use of advanced technologies in fraud detection and prevention, with particular attention to community financial institutions.

Among other issues, the study would address barriers to adoption, including cost, vendor concentration, interoperability constraints, regulatory uncertainty, data access limitations, and liability concerns. The study would require recommendations to ensure regulatory guidance is appropriately tailored to avoid discouraging adoption by smaller community financial institutions.

ICBA supports this legislation and appreciate recognition of the unique challenges faced by community banks.

Other Legislation

The SCAM Act (H.R. 7548)

While this legislation is outside the jurisdiction of this committee, ICBA thanks Representatives Meuser and Correa for introducing the ***Safeguarding Consumers from Advertising Misconduct (SCAM) Act (H.R. 7548)***.

This legislation would require online platforms to implement measures to prevent fraudulent and deceptive ads, strengthen accountability, and step up enforcement of consumer protection laws. These reforms would have a real impact in reducing online scams and protecting American consumers and could have stopped some the scams my customers experienced.

The failure to regulate online platforms for fraud in the way that banks are only exposes banks to more fraud. The stories I share above vividly illustrate that. To effectively combat fraud, we must shore up all vulnerabilities in the ecosystem. H.R. 7548 would begin to do so.

Closing

Community banks are uniquely positioned to prevent, detect, and mitigate fraud and scams and take this role very seriously. As relationship bankers, community banks know their customers in real and meaningful ways. These relationships promote access to services, prevent fraud on the front lines, and give customers a personal resource when they fall victim to fraud or scams.

Thank you again for convening today's hearing to highlight financial threats to American families, small businesses, and community banks. We appreciate the opportunity to provide community bank perspectives and hope to provide ongoing input as solutions are developed.

I look forward to your questions.