AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

FIGHTING FRAUD ON THE FRONT LINES: CHALLENGES AND OPPORTUNITIES FOR FINANCIAL INSTITUTIONS

HEARING

BEFORE THE

SUBCOMMITTEE ON FINANCIAL INSTITUTIONS

OF THE

COMMITTEE ON FINANCIAL SERVICES U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED NINETEENTH CONGRESS

SECOND SESSION

MARCH 5, 2026

Serial No. 119–60

Printed for the use of the Committee on Financial Services



www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
63–967 PDF WASHINGTON : 2026

HOUSE COMMITTEE ON FINANCIAL SERVICES

FRENCH HILL, Arkansas, *Chairman*

BILL HUIZENGA, Michigan, *Vice Chairman*
FRANK D. LUCAS, Oklahoma
PETE SESSIONS, Texas
ANN WAGNER, Missouri
ANDY BARR, Kentucky
ROGER WILLIAMS, Texas
TOM EMMER, Minnesota
BARRY LOUDERMILK, Georgia
WARREN DAVIDSON, Ohio
JOHN W. ROSE, Tennessee
BRYAN STEIL, Wisconsin
WILLIAM R. TIMMONS, IV, South Carolina
MARLIN STUTZMAN, Indiana
RALPH NORMAN, South Carolina
DANIEL MEUSER, Pennsylvania
YOUNG KIM, California
BYRON DONALDS, Florida
ANDREW R. GARBARINO, New York
SCOTT FITZGERALD, Wisconsin
MIKE FLOOD, Nebraska
MICHAEL LAWLER, New York
MONICA DE LA CRUZ, Texas
ANDREW OGLES, Tennessee
ZACHARY NUNN, Iowa
LISA McCLAIN, Michigan
MARIA SALAZAR, Florida
TROY DOWNING, Montana
MIKE HARIDOPOLOS, Florida
TIM MOORE, North Carolina

MAXINE WATERS, California, *Ranking Member*
SYLVIA R. GARCIA, Texas, *Vice Ranking Member*
NYDIA M. VELÁZQUEZ, New York
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
DAVID SCOTT, Georgia
STEPHEN F. LYNCH, Massachusetts
AL GREEN, Texas
EMANUEL CLEAVER, Missouri
JAMES A. HIMES, Connecticut
BILL FOSTER, Illinois
JOYCE BEATTY, Ohio
JUAN VARGAS, California
JOSH GOTTHEIMER, New Jersey
VICENTE GONZALEZ, Texas
SEAN CASTEN, Illinois
AYANNA PRESSLEY, Massachusetts
RASHIDA TLAIB, Michigan
RITCHIE TORRES, New York
NIKEMA WILLIAMS, Georgia
BRITTANY PETTERSEN, Colorado
CLEO FIELDS, Louisiana
JANELLE BYNUM, Oregon
SAM LICCARDO, California

Ben Johnson, *Staff Director*

SUBCOMMITTEE ON FINANCIAL INSTITUTIONS

ANDY BARR, Kentucky, *Chairman*

BARRY LOUDERMILK, Georgia, *Vice Chairman*
BILL HUIZENGA, Michigan
ROGER WILLIAMS, Texas
JOHN W. ROSE, Tennessee
WILLIAM R. TIMMONS IV, South Carolina
RALPH NORMAN, South Carolina
DANIEL MEUSER, Pennsylvania
YOUNG KIM, California
BYRON DONALDS, Florida
SCOTT FITZGERALD, Wisconsin
MIKE FLOOD, Nebraska
MONICA DE LA CRUZ, Texas
TIM MOORE, North Carolina

BILL FOSTER, Illinois, *Ranking Member*
NYDIA M. VELÁZQUEZ, New York
GREGORY W. MEEKS, New York
DAVID SCOTT, Georgia
BRAD SHERMAN, California
AL GREEN, Texas
JUAN VARGAS, California
SEAN CASTEN, Illinois
STEPHEN F. LYNCH, Massachusetts
JOYCE BEATTY, Ohio
CLEO FIELDS, Louisiana

C O N T E N T S

Thursday, March 5, 2026

OPENING STATEMENTS

	Page
Hon. Andy Barr, Chairman of the Subcommittee on Financial Institutions, a U.S. Representative from Kentucky	1
Hon. Bill Foster, Ranking Member of the Subcommittee on Financial Institutions, a U.S. Representative from Illinois	3

STATEMENTS

Hon. French Hill, Chairman of the Committee on Financial Services, a U.S. Representative from Arkansas	4

WITNESSES

Mrs. Gay Dempsey, Chief Executive Officer, Bank of Lincoln County, on behalf of The Independent Community Bankers Of America (ICBA)	5
Prepared Statement	8
Mr. Patrick McDade, Senior Vice President for Fraud and Technology Risk Management, Everbank, on behalf of The Consumer Bankers Association (CBA)	22
Prepared Statement	24
Ms. Kate McKune, General Counsel, Park Community Credit Union, on behalf of America's Credit Unions (ACU)	42
Prepared Statement	44
Mr. Joseph J. Schuster, Partner, Ballard Spahr LLP	61
Prepared Statement	63
Mr. Adam Rust, Director of Financial Services, Consumer Federation of America (CFA)	91
Prepared Statement	93

APPENDIX

MATERIALS SUBMITTED FOR THE RECORD

Hon. Barry Loudermilk:	
American Securities Association	146
Hon. Young Kim:	
American Financial Services Association	150
SIFMA	152
Hon. Al Green:	
"Melania Trump's meme coin architects accused of pump-and-dump fraud in lawsuit"	155
"Trump meme coin down 96% as Bitcoin and meme coins slide"	157
"Firm Tied to Kristi Noem Secretly Got Money From $220 Million DHS Ad Contracts"	160
Hon. Hon. Andy Barr:	
Bank Policy Institute (BPI)	169
The Responsible Data Alliance (RDA)	172
American Land Title Association (ALTA)	175

Page

RESPONSES TO QUESTIONS FOR THE RECORD

Written responses to questions for the record from Representative Rose
Mrs. Gay Dempsey 178
Mr. Patrick McDade 182
Ms. Kate McKune 184
Mr. Joseph J. Schuster 185
Written responses to questions for the record from Representative Fitzgerald
Mrs. Gay Dempsey 189
Ms. Kate McKune 190
Mr. Joseph J. Schuster 192

LEGISLATION

H.R.——, the Transaction Risk Analytics and Collaborative Exchange (TRACE) Act of 2026 195
H.R.——, the Bank Fraud Technology Advancement Act of 2026 201
H.R.——, the Scrutinizing Transactions for Overt Payment Fraud (STOP Fraud) Act 210

FIGHTING FRAUD ON THE FRONT LINES: CHALLENGES AND OPPORTUNITIES FOR FINANCIAL INSTITUTIONS

Thursday, March 5, 2026

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS,
COMMITTEE ON FINANCIAL SERVICES,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:03 a.m., in room 2128, Rayburn House Office Building, Hon. Andy Barr [chairman of the subcommittee] presiding.

Present: Representatives Barr, Hill, Huizenga, Williams, Loudermilk, Rose, Timmons, Meuser, Kim, Fitzgerald, Flood, De La Cruz, Moore, Hill, Foster, Waters, Scott, Sherman, Green, Vargas, Casten, Lynch, and Beatty.

Chairman BARR. The Subcommittee on Financial Institutions will come to order.

Without objection, the chair is authorized to declare a recess of the committee at any time.

Today's hearing is titled "Fighting Fraud on the Front Lines: Challenges and Opportunities For Financial Institutions."

Without objection, all members will have five legislative days within which to submit extraneous materials to the chair for inclusion in the record.

I now recognize myself for 4 minutes for an opening statement.

OPENING STATEMENT OF HON. ANDY BARR, CHAIRMAN OF THE SUBCOMMITTEE ON FINANCIAL INSTITUTIONS, A U.S. REPRESENTATIVE FROM KENTUCKY

Good morning.

Today's hearing continues this committee's work to combat the growing threat of financial fraud and scams harming American families, seniors, and small businesses across our country.

Fraud and scam losses are not abstract statistics. They represent retirement savings wiped out, college funds drained, and small business savings accounts emptied overnight.

The scope of the problem is staggering. According to the Federal Bureau of Investigation (FBI), Americans reported $16.6 billion in cybercrime losses in 2024, a 33 percent increase over the prior year.

Criminals are becoming more sophisticated, leveraging artificial intelligence, voice cloning, spoofed caller IDs, fake investment platforms, and coordinated money mule networks. They are exploiting

social media platforms, telecommunications infrastructure, and cross-border networks to deceive Americans at scale.

Yet, even as these schemes often originate outside the financial system—and frequently outside our borders—banks and credit unions are often the last lines of defense.

Financial institutions of all sizes are devoting substantial resources to fight fraud and scams. They are investing heavily in data analytics, machine learning, and artificial intelligence to detect suspicious activity within milliseconds. They are deploying real-time transaction alerts and customer education campaigns to encourage their customers to remain vigilant and spot common flags before funds have left their accounts.

Community banks and credit unions, despite having fewer resources, are stepping up with employee training, enhanced check verification procedures, and partnerships with local and national law enforcement.

The Trump Administration has also taken significant steps to address this escalating problem. President Trump's executive order, "Modernizing Payments to and from Americans' Bank Accounts," directs Treasury to transition away from paper checks, which are far more susceptible to theft and alteration, and toward more secure electronic payments. This shift will help safeguard Americans' tax refunds and benefits while protecting taxpayer dollars from criminal activity.

President Trump has also removed barriers to American leadership in artificial intelligence, recognizing that innovation is essential if we are going to outpace technologically savvy criminals but despite these efforts, serious structural challenges remain.

First, our legal framework for information sharing is outdated. Fraud today is networked, cross-institutional, and real-time.

Yet privacy statutes, antitrust concerns, and uncertainty under consumer reporting laws limit the ability of financial institutions to share data in ways that could identify mule networks and coordinated fraud patterns.

Second, funds availability rules under Regulation CC were written for a very different era when the primary risk was banks holding checks too long, not criminals exploiting mandatory next-day availability to drain accounts before investigations can detect fraud.

Third, our financial regulators often lack robust understanding of artificial intelligence and machine learning, preventing the establishment of clear guardrails for financial institutions.

With well-defined expectations, financial institutions will be better positioned to confidently adopt these technologies or partner with innovative third parties to more effectively detect and prevent fraud.

Last, law enforcement faces real constraints, including insufficient penalties for fraudsters, limited resources, and lack of coordination between Federal and local officials.

At the same time, we must also guard against proposals that could unintentionally fuel more scams.

Placing liability on financial institutions when a customer mistakenly authorizes a payment or transfer—often referred to as scams—does not address the underlying root causes of scams and

could worsen the problem by increasing instances of first-party criminal activity.

It would also impose significant financial strain on smaller banks and credit unions which lack substantial profits needed to absorb large scam-related losses.

Our focus today is straightforward: How do we empower financial institutions to better deter, detect, and mitigate fraud without creating perverse incentives or unintended harm?

I look forward to hearing from our witnesses and working with my colleagues to strengthen our Nation's defenses against financial fraud and scams.

With that, I yield back.

Chairman BARR. I now recognize the ranking member of the subcommittee, Dr. Foster, for 4 minutes for an opening statement.

OPENING STATEMENT OF HON. BILL FOSTER, RANKING MEMBER OF THE SUBCOMMITTEE ON FINANCIAL INSTITUTIONS, A U.S. REPRESENTATIVE FROM ILLINOIS

Mr. FOSTER. Thank you, Chair Barr, and to our witnesses.

Today's hearing continues this committee's bipartisan focus on solutions to counter the growing threat of fraud and scams facing American consumers and financial institutions.

Federal agencies, including the FBI and Federal Trade Commission (FTC), and numerous nongovernmental organizations have increased their focus on frauds and scams in recent years.

In each report, it is made clear that scams and losses from fraud are growing year after year as scams are moving online and perpetrators are becoming more sophisticated.

As Chair Barr noted, the FBI's last Internet Crime Report in 2024 reported losses of a staggering $16.6 billion from cyber-enabled scams and fraud. During coronavirus disease (COVID), the U.S. taxpayer lost well over $100 billion to scams and identity scams.

When encompassing offline activity like check fraud and information from victims that choose not to report their losses, the number is actually much greater.

Today, we are going to be discussing what can be done to support community banks and credit unions which often find themselves as the last line of defense between consumers and scammers. We will discuss what more financial institutions, and this committee can do to fight scams and fraud, the role agencies outside of our jurisdiction should play, and actions that can be taken by other industry sectors to eliminate common vectors for these activities.

Old school fraud persists, like check fraud, while scammers are quickly adopting new tools, like artificial intelligence and deepfakes, to more effectively falsify documents, impersonate consumers, or create false pretenses that trick Americans into sending their hard-earned money to bad actors.

Specifically, I worry about the role of impersonation and identity fraud in the scam system.

In 2024, the Financial Crimes Enforcement Network, FinCEN, published a report identifying more than 1.6 million Suspicious Activity Reports implicating more than $212 billion in transactions as linked to concerns with identity verification.

I would like to thank Congressman Sessions for his partnership on H.R. 7270, the Stop Identity Fraud and Identity Theft Act of 2026, which would help States build the necessary infrastructure to offer a voluntary form of digital identification for Americans that want it.

Digital identity tools are proven to be more secure and privacy preserving than physical documents in an online environment, and our bill would make important steps to provide peace of mind to Americans who worry that the person on the other end of the line may not be who they claim to be.

It is essential to also recognize the role that the Consumer Financial Protection Bureau played in countering fraud and scams, particularly for our servicemembers and older Americans.

The Consumer Financial Protection Bureau (CFPB) long served as a resource for Americans affected by these criminals, providing assistance and operating their Consumer Complaint Data base which provides important data regarding the types of scams and other illegal activities facing the public.

This work is important, and this committee should put pressure to restore the CFPB so that it can continue that important work.

Many members of this committee recognize that congressional efforts to counter fraud and scams cannot stop at the walls of this committee. Telecom service providers and social media platforms are common avenues for scammers to reach consumers.

Fighting scams require an all-of-government approach to be successful, and we should recognize that. Many times, much of the damage has been done by the time the consumer contacts the financial institution.

Technological solutions, improved information-sharing arrangements, and stronger Federal coordination provide a start to address these issues.

So I look forward to hearing the views of our witnesses on these topics.

I yield back.

Chairman BARR. The gentleman yields back.

I now recognize the chairman of the full committee, Mr. Hill, for 1 minute for an opening statement.

STATEMENT OF HON. FRENCH HILL, CHAIRMAN OF THE COMMITTEE ON FINANCIAL SERVICES, A U.S. REPRESENTATIVE FROM ARKANSAS

Chairman HILL. Thank you, Chairman Barr.

This is Consumer Protection Week, and I think I want to commend you and Dr. Foster for holding this important hearing.

Fraud and scams are not a new challenge, but the scale and complexity of the problem, as Bill just outlined, are increasing rapidly, imposing greater costs on both American families and on the financial services arena and on our small businesses.

Americans reported losses of $12.5 billion in 2024, a 25 percent increase. In communities like my own in Little Rock, I hear directly from bankers, small business owners, and consumers who are grappling with check fraud, wire fraud, and increasingly sophisticated digital scams. In our family, we have been the victim of check fraud ourselves.

Our banks and credit unions serve on the front lines of this fight, working every day to safeguard their customers, and we need an all-of-government approach. That is why I commend the work of this committee.

I yield back.

Chairman BARR. Thank you, Mr. Chairman. I commend your work as well and your focus on this issue along with Mr. Meuser, the chairman of our Oversight Subcommittee.

Today, we welcome the testimony of Mrs. Gay Dempsey, the CEO of the Bank of Lincoln County, Tennessee, here on behalf of the Independent Community Bankers of America.

Mr. Patrick McDade, the senior vice president for fraud and technology risk management at EverBank, here on behalf of the Consumer Bankers Association.

Ms. Kate McKune, the general counsel of Park Community Credit Union in the great Commonwealth of Kentucky, here on behalf of America's Credit Unions.

Kate and I have been friends for a long time.

So it is great to see you in front of our committee, Kate.

Mr. Joseph Schuster, a partner at Ballard Spahr and Mr. Adam Rust, the director of financial services at the Consumer Federation of America.

We thank each of you for taking the time to be here. Each of you will be recognized for 5 minutes to give an oral presentation of your testimony. Without objection, your written statements will be made part of the record.

Mrs. Dempsey, you are now recognized for 5 minutes for your oral remarks.

STATEMENT OF GAY DEMPSEY, CHIEF EXECUTIVE OFFICER, BANK OF LINCOLN COUNTY, ON BEHALF OF THE INDEPENDENT COMMUNITY BANKERS OF AMERICA (ICBA)

Mrs. DEMPSEY. Chairman Barr, Ranking Member Foster, and members of the subcommittee, I am Gay Dempsey, the CEO of the Bank of Lincoln County located in Fayetteville, Tennessee. We are a $225 million bank in southern-middle Tennessee bordering Alabama.

I am a member of the Board of Directors for ICBA and a member of the Fraud and Scams Task Force. I am also actively involved in the Tennessee Bankers Association where I am soon to be chairman.

I testify today on behalf of ICBA and thousands of community banks across our country. Thank you for convening today's hearing.

I am a lifelong community banker, and I have witnessed firsthand the impact of fraud on our customers and community and have seen the financial ruin that fraud can produce.

Community banks like mine are on the front lines, spending significant time and resources to educate customers and identify and mitigate fraud but coordination among financial institutions, law enforcement, and government at every level is necessary to combat this urgent problem.

My written statement contains legislative and regulatory recommendations, but I must stress that additional mandates on community banks would only harm our ability to fight fraud. I also

provide a number of stories to illustrate the impact of check fraud, imposter scams, and other schemes.

In recent years, we have seen a significant rise in check fraud. A common thread in these cases is a failure of mail security and a depositing bank that ignored red flags on account opening and accepting deposits of stolen checks for fake companies.

In some cases, lost funds were recovered after much effort and delay. In others, we had to absorb the losses.

We have also seen a rise in imposter scams enabled by unregulated social media platforms and bitcoin ATMs.

Our bank had an elderly customer with no family who fell victim to a romance scam and sold her house for $85,000. Spotting the red flags, we refused her request to wire the money to the scammer and tried our best to convince her that she was a victim, even showing her FBI reports.

In the end, we could not refuse her request to make a cash withdrawal, which she deposited in a nearby bitcoin ATM and transferred to the scammer.

This was heartbreaking, a preventable crime enabled by the use of fake social media accounts.

The Safeguarding Consumers from Advertising Misconduct (SCAM) Act, introduced by Representatives Meuser and Correa, would begin to hold social media platforms accountable for fraud like this.

Fraud losses disproportionately impact community banks relative to our asset size. For a bank like ours, fraud fundamentally impacts our ability to serve our local community.

Beyond the significant dollar losses, fraud is increasingly absorbing focus and attention, stealing valuable time that we should be spending with our customers but maybe more dangerous is the intangible impact: the erosion of consumer trust in all banks. This ironically leads consumers to seek out unregulated nonbank alternatives that put them at even greater risk.

Community banks are built on strong relationships. This sets us apart from larger transaction-oriented banks, and fraud jeopardizes these critical relationships.

Given these high stakes, how are community banks responding?

First, we are investing significant amounts in technology, including AI, to detect fraud. These tools, which are important but not foolproof, add significant cost for our bank.

One of the draft bills before this committee, the Bank Fraud Technology Advancement Act, would require a comprehensive agency study of the use of AI in fraud prevention. This study would be valuable.

Second, we train our staff to spot fraud and report suspicious activity. Our staff are the point of contact and positioned to detect fraud early and intervene. Their training is critical, but so are the personal relationships and the knowledge they have. In our close-knit community, they are truly the first line of defense.

At the industry level, Independent Community Bankers of America (ICBA) created a Fraud and Scams Task Force that shares information and best practices, meets with regulators, and develops resources for our peers.

My statement also contains recommended changes to Fed Regulation CC, which governs check clearance. This, along with the draft Scrutinizing Transactions for Overt Payment Fraud (STOP Fraud) Act, would help community banks mitigate check fraud by providing more flexible hold times.

Finally, a third draft bill before this committee, the Transaction Risk Analytics and Collaborative Exchange (TRACE) Act, would expand critical information sharing while providing safe harbors.

Thank you for your work on the draft bills and for convening today's hearing.

[The prepared statement of Mrs. Dempsey follows:]

ICBA
One Mission. Community Banks.®

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.

866-843-4222
icba.org
1100 New York Avenue NW
Suite 500 East
Washington, DC 20005
518 Lincoln Road
P.O. Box 267
Sauk Centre, MN 56378

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 myself 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.

Mail theft and check alteration

In 2022, a small business customer of ours had approximately 15-20 checks stolen from the mail and altered, totaling almost $600,000. The vast majority of these checks were mobile deposited over a period of time at several larger banks. The window for returning checks is midnight of the next banking day. However, the business maintains high balances at BOLC and understandably did not notice the posting of the 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.

Bank of Lincoln County gave our customer immediate credit for the checks as soon as the alterations were discovered and began the arduous process of recovering the funds. We returned the checks through the Federal Reserve claiming "Breach of Warranty," a claim that is exempt from the midnight return window. The bank of first deposit had accepted an altered check, a clear breach of warranty.

A critical piece of this story is that, 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.

We pursued our case, citing UCC law, again, with the mediation of the Fed, 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 harder for us to serve our community.

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 by an LLC created in Georgia expressly for the purpose of perpetuating a fraud. (We later found out that the fraudster had opened and closed a series of LLCs in Georgia and had no physical office, which should have been an obvious red flag to the depositing bank.) We discovered the alteration within five days; however, the fraudster had promptly withdrawn the majority of the funds.

We returned the check as a "breach of warranty"—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. (ICBA and community banks have been asking the UCC Permanent Editorial Board to revisit and modernize the definitions of counterfeit and altered, which were written before today's digital alteration techniques existed.)

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 reached out to the Tennessee Bankers Association to see if they had a contact. When I finally identified someone at the large bank who could supposedly help, he responded to our first email and then went silent when he learned what the issue was concerning. It was beyond frustrating.

We hired a lawyer since it was, to us, such a large amount. In 2025, an "expert" claimed it was counterfeit under the current definition. Borders and minute security language had been digitally altered which you would not catch with a usual observance of the check. 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. I learned about ten months into this process that the fraudulent account had $11,000, which the large bank had withheld from us. After three requests, the bank of first deposit returned the $11,000 to our bank over a year after the incident occurred. All parties should be held to full transparency.

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, which highlights so 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 without 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 it was a scam, 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 and trap a 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,

[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

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.

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.

Chairman BARR. Thank you.

I now recognize Patrick McDade for 5 minutes.

STATEMENT OF PATRICK McDADE, SENIOR VICE PRESIDENT FOR FRAUD AND TECHNOLOGY RISK MANAGEMENT, EVERBANK, ON BEHALF OF THE CONSUMER BANKERS ASSOCIATION (CBA)

Mr. MCDADE. Chairman Barr, Ranking Member Foster, and members of the subcommittee, thank you for the opportunity to testify.

My name is Patrick McDade, and I am the senior vice president for fraud and technology risk management at EverBank.

Before joining EverBank, I spent over a decade as a State and Federal prosecutor. I also serve as the chair of the Consumer Bankers Association's Fraud Management Committee.

The CBA's broad membership has long been raising the alarm about the rise in fraud and scams that are inflicting deep financial and emotional harm on American consumers and small businesses.

Banks invest billions of dollars and millions of hours to combat fraudsters and scammers each year. However, banks cannot face this growing threat alone.

In 2024, the FBI received more than 850,000 Internet Crime Complaint Center (IC3) complaints involving losses of over $16 billion, which was a 33 percent increase over 2023.

However, while consumers expect a meaningful response to these complaints, Government Accountability Office (GAO) reports have revealed a lack of coordination among Federal bodies to assist victims and prevent frauds and scams.

Meanwhile, the criminals behind these frauds and scams are using AI, social media, and dark web platforms to coordinate with each other and improve their attacks and techniques.

Historically, fraudsters have attacked the financial services industry through traditional bank fraud methods: identity theft, forging or altering checks, wire fraud, et cetera.

More recently, these criminals have focused on emerging digital bank platforms, fraudulently accessing accounts online and making unauthorized payments.

Banks hardened their digital controls, developed data-focused fraud tools, and strengthened digital security to combat these emerging threats.

In response, today the criminals are focused on a new tactic: Scams directed at our customers.

Frauds and scams are often conflated, as both use complex schemes and deceptions to steal. However, it is important to understand the differences between frauds and scams.

The key differences are who is being deceived and who is authorizing the transactions.

As I described, in bank fraud, the criminals are trying to deceive the bank and fraudulent transactions are sent.

With scams, however, the criminal is not deceiving the bank—they are deceiving the customer. The customer believes they urgently need to move money to invest, to help a loved one, or to avoid a penalty. The customer then contacts the bank and authorizes a transaction to move money.

Banks work hard to protect their customers in the Main Street communities they serve from these scams. Banks monitor unusual activity, educate customers about fraud and scams, and train their staff to recognize red flags that indicate a customer may be a scam victim.

Banks are doing what they can do to stop scams, but there are several important steps that policymakers can take to help.

First, the Federal Government should establish a national strategy to combat fraud and scams. Because so much of the activity involving scams originates from social media, telecommunications, and other places outside the financial sector, this strategy must include cross-industry engagement.

One step toward accomplishing this could be an executive order that includes unified coordination with the private sector. While my written testimony provides more detail, such an order could establish a centralized interagency reporting and data-sharing infrastructure to streamline complaint intake and response. This would provide immediate structural alignment across agencies while longer-term legislative reforms are developed.

To that end, CBA strongly supports many bipartisan and bicameral efforts, including the leadership of Representative Nunn through the Guidelines for User Age-Verification and Responsible Dialogue (GUARD) Act and the Taskforce for Recognizing and Averting Payment Scams (TRAPS) Act, Representative Meuser through the SCAM Act, and other efforts, such as Representative Kim's No More Shielding Corruption and Misuse in Spending (SCAMS) Act. These represent important steps in cross-agency coordination.

Congress should also expand safe harbor protections so financial institutions can share real-time fraud and scam threat intelligence without undue legal risk.

Federal regulatory frameworks must also be modernized, including Reg CC.

Customer education is equally vital. Banks commit significant resources to educate their customers about fraud and scams, but a national fraud and scam awareness campaign would make a substantive difference.

Finally, fraud and scams are currently reported to the government through FinCEN's suspicious activity reporting process. Transitioning to a modern fraud signal report would lead to more valuable and actionable data-gathering by the government.

The fraud and scam epidemic confronting American consumers is not a series of isolated incidents. It is a rapidly evolving, technology-accelerated global threat that inflicts billions of dollars in losses each year and affects millions of Americans in every district and Main Street consumers across the country.

Thank you, and I look forward to your questions.

[The prepared statement of Mr. McDade follows:]



Testimony of Patrick McDade

Senior Vice President, Fraud Risk and Technology Risk Management,
Head of Internal Investigations

EverBank N.A.

U.S. House Financial Services Committee

Financial Institutions Subcommittee

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

March 5, 2026

Chairman Barr, Ranking Member Foster, and Members of the Subcommittee, thank you for the opportunity to testify today. My name is Patrick McDade, and I am Senior Vice President, Fraud Risk and Technology Risk Management, Head of Internal Investigations at EverBank.[1] Prior to joining EverBank, I spent over a decade as a state and federal prosecutor, bringing an understanding of regulatory expectations, corporate governance, and financial crime expertise to my role at the bank.

In addition to my role at EverBank, I also serve as the Chair of the Consumer Bankers Association (CBA)[2] Fraud Management Committee. The CBA Fraud Management Committee provides senior leaders of fraud and scam prevention at the nation's leading retail banks an open forum to discuss best practices, emerging trends, and provide expertise related to advocacy in the federal legislative and regulatory environment.[3] On behalf of the CBA Fraud Management Committee, I also served as a delegate to the Aspen Institute's National Taskforce on Fraud and Scam Prevention.

CBA's broad membership – representing America's leading Main Street banks - have been raising the alarm for years about the rise in fraud and scams that are inflicting deep financial and emotional harm on American consumers and small businesses. Banks invest billions of dollars and thousands of hours to combat fraudsters and scammers each year.[4] This includes constant education campaigns to warn customers about new and emerging threats.

Successfully combating fraud and scams requires a robust understanding of the key differences between the two illicit activities, as their unique features should dictate the methods used to counter each of them. Bank fraud generally involves an attempt to obtain money that is owned by or under the custody or control of a financial institution by false pretenses or misrepresentation, or at a more basic level, attempts to defraud a financial institution See: (18 US Code Sec. 1344). This generally refers to situations in which a fraudster tries to borrow, withdraw, or move money from a bank account without the authority to do so. In modern times this often involves trying to use a computer system to access a customer's account without authorization or impersonate a customer through the phone channel. Bank fraud is best prevented

---

[1] EverBank N.A., formerly known as TIAA Bank, is a nationwide specialty bank servicing clients across the United States with a focus on delivering high-value products competitive deposit, lending, and commercial solutions.
[2] The CBA is a member-driven trade association, and the only national financial trade group focused exclusively on retail banking—banking services geared toward consumers and small businesses. As the recognized voice on retail banking issues, CBA provides leadership, education, research, and federal representation for its members. CBA members operate in all 50 states. They include the nation's largest bank holding companies as well as regional and super-community banks. Eighty-three percent of CBA's members are financial institutions holding more than $10 billion in assets.
[3] https://consumerbankers.com/committee/fraud-management-committee/
[4] https://www.pymnts.com/fraud-prevention/2023/banks-and-payment-firms-tap-ai-to-combat-fraud-amid-surge-in-sophisticated-financial-crime/

with controls that detect when a misrepresentation occurs, and banks with online presences have established strong control environments to detect and prevent these types of fraud attempts, securing the customers' assets and protecting the integrity of the financial system.

Scams, on the other hand, involve criminals deceiving customers directly, often through phone, text, or online communication and convincing the bank's customers to send money out of the bank under false pretenses. Notably, scams generally occur outside of the bank's control environment and the first time the bank becomes aware of the transaction is when the customer requests that their money be moved. Like bank fraud, scams, are best prevented where the deception occurs – in the phone, text, or online channel where the scammer tries to convince the customer to send them money. Today, the primary tool we have to help our customers recognize and prevent scams is to raise consumer awareness of these activities beyond their banking channels and that target the fraudulent conduct occurring in those external channels.

This distinction between fraud and scams is critical and is one reason that CBA has called for consistent standards for how various fraud or scams are classified. On fraud, banks continue to deploy significant controls to prevent and detect fraud, deploying behavioral biometrics, artificial intelligence models, real-time transaction screening, two-factor authentication, digital ID verification, dark web monitoring, and 24/7 investigative teams. The results matter: Most fraud attempts are stopped before customers ever see them.

Banks invest heavily to fight fraud, working together with government and fraud prevention experts leverage data and signal to detect and prevent billions of dollars of fraud within bank-managed channels. When fraud touches the bank, we can see it, detect it, and stop it.

Scams are fundamentally different. Scams occur when criminals manipulate victims into willingly authorizing payments. Banks are required to direct authorized payments where the customer wishes them to go. These are not bank system breaches that the banks are capable of detecting and preventing, but are social engineered operations aimed at the customer or small business where the deception and related data and signals happen entirely outside the regulated banking system. Only when the customer authorizes a payment does the bank get involved, and then it is often too late.

Unfortunately, both fraud and scams have continued to become more sophisticated and more pervasive year-over-year. Criminals are leveraging data from decades of breaches and stolen information to carefully target potentially vulnerable scam victims. They are imitating legitimate individuals, companies, and financial institutions to gain the trust of our customers. They are eroding trust in reputable institutions, inflicting financial and emotional harm on our customers, and exploiting some of the most vulnerable members of our society.

Scams are largely driven by criminals operating on social media platforms, online marketplaces, messaging apps, telecom networks, and fraudulent digital advertising channels among other places. New technology has birthed new forms of scams, especially in the AI era. These criminal enterprises relentlessly bombard consumers outside of bank-managed channels, with sophisticated scams through endless phishing emails, spam texts, fake "Amazon shipment" notifications, long-term interpersonal engagements on social media platforms, and more. Continuing technological evolutions are making it harder for even the most diligent consumers to effectively be on their guard. Scammers are using AI to assemble detailed profiles on potential scam victims, obtaining details they use to establish trust. More advanced applications like AI-generated voice cloning and video impersonations, once confined to the realm of science fiction, are now a fraud and scam reality. Although many of the schemes are not new, modern scams evolve every day. Unfortunately, as the deception happens so far upstream, banks are often the last line of defense with scams, not the first. By the time a bank is involved, the customer is already convinced that they need to send money to the scammer, and the bank is trying to put the puzzle together while the customer insists that the money be sent right away.

CBA members – and the banking industry as a whole - are working day and night to combat the swift and nimble nature of these criminals. To win the fight, however, and actually stop fraud before it even reaches a bank or a bank's customer, there are several opportunities for policymakers to make a meaningful difference. The steps this Committee and specific members have taken in a bipartisan manner demonstrate policymakers' aim to tackle this consumer crisis. A number of legislative proposals have been introduced and will be extremely meaningful to address the numerous complicated facets of scams. But even more will be needed, including Administrative and agency actions to create an even greater unified approach across government and the private sector to educate consumers, to investigate and mitigate scams, and prosecute bad actors. Overall, the efforts by Congress and the Administration should be aimed at: strengthening coordination; enhancing information sharing; modernizing regulatory tools; a unified approach to scam awareness education and; protecting consumers when and where the scam occurs, before it ever reaches their bank accounts.

In my testimony I will:

- Provide an overview of the alarming scale of the fraud and scam epidemic
- Outline the differences between fraud and scams that impact the toolsets used to address each
- Explore why scammers are winning
- Highlight what banks are doing to protect customers
- Emphasize the need for a whole-of-government strategy to combat fraud and scams
- Recognize positive federal legislative and regulatory developments
- Offer recommendations and a roadmap for policymakers to better support the private sector and federal government in stopping fraud and scams

EverBank and the Consumer Bankers Association's membership more broadly remain committed to working with this Committee to increase public and private sector coordination, better protect consumers, and address the root causes of fraud and scams.

A National Crisis: The Alarming Scale of the Fraud and Scam Epidemic in the U.S.

According to recent Federal Trade Commission (FTC) data, consumers reported losing approximately $12.5 billion to fraud in 2024, which represents a twenty-five percent increase from the previous year. This trend is just due to a spike in reporting, we are seeing a significant rise in the percentage of Americans who have fallen victim to fraud or scams, jumping from twenty-seven percent thirty-eight percent from 2023 to 2024.[5]

But, as noted earlier, scams have become far more pervasive for consumers—and as the FTC reports what acts comprised those $12.5 billion in losses, the top five are all scam activity, including: 1) imposter scams; 2) online shopping and negative review scams; 3) business and job opportunity scams; investment scams; and internet service scams.

As the FTC reports, "big losses follow scams that start with a call or on social media"[6] This economic damage is inextricably linked to the profit incentives of the digital platforms where these schemes frequently originate.

An internal report from one of the most prominent online platforms estimated it generated 10% of its revenue, or $16 billion, by allowing fraudulent advertisements and scams to proliferate on their websites.[7] That same platform is also accountable for close to half of the reported scams on the peer-to-peer payment platform Zelle, leading to millions in losses for customers.[8] While certain online platforms profit, the banking industry faces the burden of managing the fallout.

Scammers often operate across international borders and exploit digital platforms with limited identify verification. The challenge is further complicated by a fragmented reporting infrastructure that obscures the true extent of the crisis. While the Federal Bureau of Investigation (FBI) received nearly 589,400 scam related complaints in 2023 totaling over $10.55 billion dollars in losses, a recent Government Accountability Office (GAO) report reveals a systemic lack of coordination among federal bodies to investigate or assist victims of scams. Of the thirteen federal agencies involved in countering these threats, only eight currently maintain the capacity to receive scam complaints from the public, leaving a significant portion of the regulatory landscape unable to effectively track or respond to the evolving needs of consumers.[9]

---

[5] https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024
[6] https://www.ftc.gov/system/files/ftc_gov/images/csn-scammy-snapshot-2024.png
[7] Horwitz, J. (2025, November 6). Online Platform is earning a fortune on a deluge of fraudulent ads, documents show. Reuters.
[8] https://www.wsj.com/tech/meta-fraud-facebook-instagram-813363c8#selection-2405.0-2405.60
[9] https://www.gao.gov/assets/gao-25-107088.pdf

When scammed, victims face difficulty navigating all the service providers, law enforcement agencies and multiple jurisdictions that may be involved. Banks, realizing that they are not capable of detecting and stopping scams on their own and face regulatory obstacles when trying to, struggle to join with other industries to share information and pool resources. Law enforcement agencies have tools to counter the swift actions of illicit actors working globally, but they require new mandates, immediate access to data and signals, and resources to evolve new ways to work across silos of expertise and legal authority.

Fraud and Scams Are Related, but Distinct, Illicit Activities that are Addressed through Different Toolsets

Fraud and scams are often conflated in discourse of this threat, as both have the same net result: funds ultimately come into the possession of illicit actors and can then subsequently be used for other nefarious purposes. However, it is vital to distinguish between the two because the remedies required for stopping the two are different.

Bank fraud generally involves an attempt to obtain money that is owned by or under the custody or control of a financial institution by false pretenses or misrepresentation, or at a more basic level, attempts to defraud a financial institution See: (18 US Code Sec. 1344). This generally refers to situations in which a fraudster tries to borrow, withdraw, or move money from a bank account without the authority to do so. The term "scams" covers instances in which individuals are manipulated into authorizing transfers themselves, a category sometimes referred to as "authorized push payment fraud."

These methodologies leverage some of the same tactics, such as social manipulation and technical exploitation to bypass traditional safeguards, but there are tangible differences. For example, interpersonal and social deceptions such as romance scams, often termed "pig butchering," represent a form of long-term engagement where bad actors cultivate false intimacy over months to induce victims into making authorizing investments or emergency transfers. Here these methodologies are used to facilitate a "scam," to convince the victim to push out funds to the criminal themselves.

However, similar tactics are employed in job scams where synthetic professional identities are used to harvest personal data and bank details from unsuspecting job applicants under the guise of legitimate remote employment. The same methodologies are also used for the purpose of fraudulently gaining access to a victim's account. Furthermore, despite the decline of physical paper in commerce, check fraud remains a significant risk involving either fake checks designed to trigger advance fee repayments or check washing where stolen mail is altered to divert funds. The rise in remote deposit capture and using cell phone photos to deposit checks through apps creates further difficulties as banks do not have the physical check to examine when determining

whether an instrument is altered or forged. This sits alongside broader bank transfer fraud which leverages both fraud attacks on banks' digital controls and social engineering to bypass standard verification protocols.

This distinction matters because the tools most effective in combating fraud and scams will necessarily differ based on these features. With respect to fighting fraud, since the illicit activity centers on impermissibly gaining access to a victim's account, the necessary tools are those that ensure authorized access, with particular emphasis on confirming the identity of the person attempting to access the account. Through tools such as password protection, multi-factor authentication, biometrics, device risk assessment, and other advanced fraud detection methods, banks are well positioned to determine whether a transaction was truly initiated by the consumer and often can verify whether the funds are being sent to a like-named account.

With respect to fighting scams, however, the necessary toolset is entirely different and extends beyond the control environment of banks. The key issue is that, in a scam, the consumer knowingly and intentionally authorizes payment to a particular account. In many cases the customer is quite insistent that the payment be processed immediately, and the bank has very limited information as to why the customer is sending the payment to a particular destination. Banks do not have access to the upstream communications — such as emails, social media messages, text messages, video calls, or phone calls — that would provide insight into the nature and validity of the relationship prompting the consumer to initiate the transaction. The fraud detection signals exist as a part of these upstream communications, and the bank does not have access to those signals. This issue is further exacerbated as an increasing number of transactions occur outside traditional bank-enabled channels, such as through fintech enabled rails or Bitcoin ATMs, that bypass conventional protections, leaving consumers more vulnerable. Accordingly, the tools needed to combat scams must target these upstream channels through which scams are perpetrated and promote consumer education aimed at helping individuals identify and avoid such schemes. The time to detect or prevent the scam is when the deception occurs, during upstream communication. Scam education can prevent deception which is why banks work hard to educate their customers. Otherwise, the deception signals related to upstream communication are essential to disrupt the scam and banks do not have access to those signals.

How Scammers are Winning, and Why Banks Cannot Stop Them Alone

To build a truly effective defense, we must understand why scammers are currently succeeding at such a high rate. The average American is facing a constant, multi-front attack that happens largely outside the safety of bank-monitored channels. These criminals use a relentless stream of phishing emails, scam texts impersonating business and financial institutions, fake shipping alerts, follow-up phone calls, social media messages, and fake websites and social media profiles and advertisements to target people where they live and work.

The threat vectors for scams in particular is almost exclusively present on non-financial platforms where the warning signs are often obvious but go unaddressed. We see this in online platforms and marketplaces where the exact same car is listed for sale in every state at once, or on social media or dating sites where synthetic profiles send the same automated messages to thousands of potential targets. Perhaps most concerning is the rise of social media streams and pages that are openly dedicated to teaching people how to commit fraud or scams, yet these platforms often provide no clear way for the public to report the content or for the authorities to effectively shut them down.

This problem is significantly worsened by the rapid pace of technological change, which makes it difficult for even the most careful consumers to stay protected. For example, AI-powered voice cloning and image impersonation, which used to be the stuff of science fiction, is now a common tool for scammers to impersonate loved ones or officials to induce a consumer into sending funds. These criminal organizations operate across international borders and target every piece of technology we rely on, from our smartphones to our personal computers, to trick people into moving money out of the regulated financial system and into the hands of bad actors.

How Financial Institutions are Working Proactively to Safeguard Consumers

Financial institutions are deeply committed to safeguarding their customers, especially individuals who may be more vulnerable, such as older adults. This commitment extends far beyond simply meeting regulatory requirements. It reflects a genuine dedication to protecting customers' financial security, promoting their overall wellbeing, and ensuring they can engage with and conduct their financial services needs confidently and safely. Financial institutions utilize the unique tools and train passionate fraud detection and investigation teams to prevent and mitigate fraud, as well as the tools at their disposal to mitigate scams, though given the unique nature of scams, banks are only able to diminish certain risk vectors that are actually within their control.

Mid-sized and regional financial institutions like EverBank invest resources and time in specialized training for staff, purchase and integrate fraud prevention technology and implement programs designed to identify and assist at risk consumers, helping them to not fall victim to scams. Some of the techniques we use include:

- Conducting risk assessments on transactions and their destinations across payment channels
- Using behavioral biometrics to detect and prevent account takeovers

- Reporting bad actors and sharing information with consortiums and credit bureaus to mitigate scams
- Investing resources in both people and technology to combat innovative scams
- Targeted customer training for scam and fraud scheme awareness
- Collaborating with law enforcement agencies to provide fraud and scam training
- Implementing two-factor authentication
- Developing a robust taxonomy for reporting and classification to address issues effectively and at scale
- Using advanced analytics to identify and combat account takeovers
- Utilize targeted in-app messaging to inform and educate consumers
- Investigating the dark web for compromised accounts proactively to protect customers.

While not all banks have the resources of some of the largest financial institutions, we do still leverage sophisticated third-party fraud tools to protect our clients. However, banks like EverBank are often more reliant on manual processes and skilled fraud detection and investigation associates to combat fraud and scams. These fraud-fighters work directly with our customers and other financial institutions to decision fraud alerts, investigate cases, and work to recover money that was moved between institutions due to fraud or scams. By taking proactive steps, including monitoring unusual account activity, educating customers about common and emerging fraud and scam techniques, and creating policies that prioritize customer protection, banks demonstrate a sincere desire to support the Main Street communities and protect the customers they serve. Ultimately, these efforts reinforce trust, strengthen long-term customer relationships, and help create a safer financial environment for everyone across the banking ecosystem.

Many institutions the size of EverBank also leverage the resources provided by trade associations such as CBA. As previously noted, CBA's Fraud Management Committee has become a resource for member banks to discuss and share mitigation efforts, discuss types of attacks, and data trends across different institutions. Some examples about how effective this Committee has been for the industry, and the consumers we serve, examples of the action's banks are taking to fight fraud and scams, and protect their customers, include:

- Sharing best practices to combat specific scams and fraud schemes
- Identifying and sharing new fraud trends
- Establishing contacts at other banks to expedite fund recovery
- Engaging with fraud service vendors to share knowledge and improve tools
- Meeting with other industry groups such as Telecoms to share knowledge and establish best practices
- Engage with industry groups such as EWS, NACHA, to suggest improvements to protect our institutions and customers

- Bring in experts to educate the membership on new trends and emerging threats
- Sharing customer communication and training methods
- Investing resources in both people and technology to combat innovative scams to identify and combat account takeovers

While this list is not exhaustive, it demonstrates the commitment of financial institutions across the country in combating fraud and scams daily.

CBA Strongly Supports a Whole-Of-Government Approach to Combat Fraud and Scams

There is a desperate need for a greater collective approach to addressing the root causes of fraud and scams, before they ever reach a bank or, for that matter, a bank's customer.

In July 2024, CBA convened a roundtable with participants representing the federal government, private sector entities, non-profit consumer organizations, and industry trade associations from the banking and telecommunications sectors to discuss the need for a national strategy for combating fraud and scams. CBA also contributed to the publication of a discussion paper exploring how industries could work together and with government to prevent fraud and other harms against consumers and businesses, "Stopping Scams Against Consumers: Roadmap for a National Strategy."[10] These efforts were followed by the Aspen Institute Financial Security Program (Aspen FSP) announcing the formation of a National Task Force for Fraud & Scam Prevention - an initiative that brought together leading stakeholders from government, law enforcement, private industry, and civil society to develop a nationwide strategy aimed at helping prevent fraud and scams.

CBA simultaneously worked with our Fraud Management Committee and through the Aspen Institute's National Task Force for Fraud & Scam Prevention, of which I served as a delegate, to develop important industry and government wide recommendations regarding fraud and scams.[11]

Although the banking industry is working day and night to combat the swift and insidious nature of these criminals, to win the fight, and actually stop scams before they even reach a bank, there are several important steps policymakers can take. One of the most important things the federal government can do today is establish a whole-of-government strategy—one that creates a unified set of definitions and terminology for categorizing different frauds and different scams. A singular and approachable means for ensuring victims can report scams, with tracking and information systems that cut across agencies to deliver critical information to various agencies, law enforcement, and as appropriate, industry participants, such as banks.

---

[10] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4897644
[11] https://fraudtaskforce.aspeninstitute.org/phase-one-outputs

While much of the recommendations below focus on Congressional actions and recommendations, the Administration could also take meaningful steps in the near term, in tandem with Congress' actions, to initiate near-term and longer-term changes. For example, the Administration could issue an Executive Order (EO) establishing a formal, government-wide framework for combating fraud and scams. Such an Executive Order would not replace legislative action, nor would it alter Congress's important oversight role. Rather, it would provide immediate structural alignment across agencies while longer-term statutory reforms are developed and considered.

Any EO should identify an agency to lead this whole-of-government approach, and accelerate many of the bipartisan objectives already under consideration by Congress, including:

- Creating a nationally coordinated fraud scam awareness campaign, similar to the Smokey the Bear campaign to prevent forest fires or the "Take Five to Stop Fraud" campaign in the United Kingdom
- Directing the development of a unified federal fraud and scam taxonomy and standardized definitions across agencies
- Establishing a centralized inter-agency reporting and data-sharing infrastructure to streamline complaint intake and trend analysis
- Clarifying safe harbor protections to enable responsible cross-sector information sharing among financial institutions, telecommunications providers, and online platforms
- Formalizing coordination between financial regulators, law enforcement, the Federal Trade Commission, Treasury, the Department of Justice, and telecommunications regulators
- Requiring periodic public reporting on scam typologies, enforcement actions, and loss trends
- Elevating fraud and scam prevention as a core national consumer protection priority

Given the fragmented reporting structure identified by the Government Accountability Office and the cross-sector nature of scam activity, executive coordination is both practical and urgently needed.[12] Moreover, a formal whole-of-government directive would send a strong signal to criminals – both domestic and transnational – that the United States is aligning its enforcement, regulatory and supervisory tools to address scams at their source.

Emerging Positive Federal Opportunities to Combat Scams

Congress and members of this Committee should be commended for coming together in a bipartisan way to work collaboratively in the fight against fraud and scams.

[12] https://www.gao.gov/products/gao-25-107088

Positive Legislative Developments

Ongoing efforts in Congress are encouraging, particularly through bipartisan and bicameral measures such as the Guarding Unprotected Aging Retirees from Deception (GUARD) Act[13] and the Taskforce for Recognizing and Averting Payment Scams (TRAPS) Act.[14] These bipartisan bills, led by Representative Zach Nunn (R-IA) in the House, provide essential, targeted protections for elderly populations and aim to streamline interagency communication through the formation of specialized anti-fraud task forces.

More recently, the Financial Services Committee has continued to lead the charge through hearings and roundtables. This past October, under the leadership of Subcommittee Chairman Dan Meuser (R-PA), the House Financial Services Oversight and Investigations Subcommittee held an important hearing that provided a great platform to identify exactly how scammers are executing their schemes. Roundtables with industry participants have continued to build on this work.[15]

Further, additional bipartisan and bicameral legislative solutions such as the Safeguarding Consumers from Advertising Misconduct (SCAM) Act have been introduced.[16] This legislation, also led by Subcommittee Chairman Dan Meuser (R-PA) in the House, represents a concrete step toward addressing the origin of many schemes by directing the FTC to establish identity verification and safety protocols for advertisers on online platforms. This measure is particularly vital given that fraudsters often leverage deceptive advertisements to facilitate fraudulent product sales outside the banking environment, often resulting in the permanent flight of capital from the regulated financial system.

CBA strongly supports these legislative proposals, roundtables, and hearings.

CBA is also pleased that several thoughtfully drafted pieces of legislation have been included for discussion in this hearing. This includes proposals to establish a safe harbor for banks related to information sharing, to require federal bank regulators to conduct a study about the technology being used, and needed, by banks to combat frauds and scams, and to consider updates to the Regulation CC framework.

Positive Congressional Appropriations Developments

---

[13] https://www.congress.gov/bill/119th-congress/house-bill/2978
[14] https://www.congress.gov/bill/119th-congress/house-bill/4936
[15] https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=410851
[16] https://www.congress.gov/bill/119th-congress/house-bill/7548

The most recent Financial Services and General Government Appropriations bill represents a particularly significant step in the fight against fraud.

As CBA has been calling for a whole-of-government approach to fraud and scams, the package contains language directing the Department of Treasury, in consultation with all members of the Financial Stability Oversight Council (FSOC) and the Federal Trade Commission (FTC), to submit a national strategy or plan that leverages and augments local, State, and Federal resources within the financial sector to mitigate and prevent online scams.[17] We commend the Representative and Senators for recognizing the continued rise in prevalence and damage to the American consumer that we have called attention to as an industry for so long. We look forward to Treasury carrying out this language and are happy to provide any resources necessary to aid in its development.

Additionally, CBA commends the inclusion of language directing FinCEN to submit a report encapsulating many different vectors of fraud data such as the volume of scams, the number of individuals scammed, the dollar amount lost to scams, and which type of scam was employed.[18] Having this data in one clear concise report will give key insights into trends the aforementioned GAO reports state are clearly missing in its current dataset.

Despite these successes in the appropriations process, significant legislative work remains to be done.

Positive Executive Branch and Regulatory Developments

The Administration is also taking steps against the evolving fraud landscape, marked by a significant increase in engagement from the Department of the Treasury and other prudential regulators. The recent issuance of a Request for Information (RFI)[19] regarding potential actions to address payments fraud represents a critical opportunity for industry participants to shape a more cohesive regulatory framework. In submitting formal comments, CBA emphasized that any solutions must facilitate a robust cross sector and public-private collaboration. This approach ensures that all relevant stakeholders, including those in the telecommunications and social media sectors where scams often originate, bear the necessary obligations to monitor and disrupt fraudulent activity at its source.[20]

The Executive Branch has further intensified its enforcement through the Department of Justice's creation of the Scam Center Strike Force. This initiative represents a targeted response to the

---

[17] Joint Explanatory Statement, Public Law 119-75
[18] Joint Explanatory Statement, Public Law 119-75
[19] https://www.federalregister.gov/documents/2025/06/20/2025-11280/request-for-information-on-potential-actions-to-address-payments-fraud
[20] https://consumerbankers.com/comment-letter/cba-responds-to-prudential-regulator-rfi-on-payments-fraud/

proliferation of Southeast Asian scam compounds that orchestrate complex pig butchering and cryptocurrency investment schemes against Americans. By actively dismantling these criminal organizations, the Strike Force provides a vital mechanism to counter groups that have historically operated with immunity.

In addition to these strategic inquiries, the Federal Reserve has taken operational steps to bolster the nation's defenses by releasing comprehensive online toolkits for scams and check fraud mitigation.[21] These resources are designed to support broad based education and increase awareness among both financial institutions and the general public, directly addressing the reporting and education gaps previously identified by the GAO. By providing detailed information on the fundamental mechanics of fraud and the specific tactics employed by illicit actors, the toolkits enable the payments industry to better identify and counteract sophisticated schemes in real time. These initiatives foster the type of industry collaboration that is essential for mitigating the financial impact of authorized push payment fraud and modern check washing techniques.

While these educational tools represent a component of a national defense strategy, they also highlight the ongoing necessity for a unified federal approach that combines consumer awareness with robust technological safeguards. The toolkits provide essential information on various scam scenarios to heighten consumer awareness, yet the long-term effectiveness of these measures will depend on their integration into a wider national strategy that includes standardized reporting and clear legal accountability for all participants in the digital payments ecosystem. By establishing a shared baseline of knowledge and fostering cooperation across the financial sector, the Federal Reserve's initiatives serve as a foundational element in the broader effort to protect the integrity of the American financial system from increasingly innovative criminal threats.

Recommendations for Policymakers to Better Support the Private Sector and Federal Government in Stopping Fraud

This relentless threat of fraud and scams can only be effectively addressed through a comprehensive, whole-of-government approach that promotes cross-sector, public-private collaboration. A coordinated federal strategy – integrating financial regulators, law enforcement, and other relevant agencies – should prioritize fraud and scam prevention as a core component of protecting consumers' economic well-being. Importantly, the tools that this strategy prioritizes for fighting fraud and scams need to be properly calibrated for targeting and addressing the unique aspects of both. To meaningfully reduce scam losses, Congress and the Administration must improve coordination across agencies, remove barriers to information sharing, update

[21] https://www.frbservices.org/news/fed360/issues/081425/industry-perspective-toolkits-scams-check-fraud-mitigation

regulatory tools for the digital era, and shift prevention efforts upstream—stopping scams before funds ever move through the banking system.

Information Sharing

Central to these efforts is robust information sharing that enables those on the front lines to identify, target, and disrupt illicit activity. The first step in stopping a threat is recognizing it, and initiatives that facilitate the sharing of actionable information are essential. To that end, a centralized, industry-wide framework, including a common fraud and scam taxonomy and consistent terminology, is vital. A shared language and standardized reporting structure would improve transparency, strengthen accountability, and enhance the quality and comparability of data across sectors. Uniform fraud reporting standards – developed collaboratively across the banking, social media, and telecommunications industries – would further streamline investigations and improve coordinated response efforts. To enable meaningful information sharing, policymakers should also clarify and expand safe harbor frameworks to explicitly cover fraud and scams, ensuring institutions can share relevant threat intelligence with confidence and without undue legal risk. Financial institutions are eager to share this information to strengthen collective defenses, but they must be assured that doing so will not expose them to unnecessary liability.

Fraud and scams are currently reported to the government through the FinCEN Suspicious Activity Reporting process. This process was designed for AML/BSA reporting that is typically retrospective and built around analyzing transactional data to evaluate potential money laundering which is submitted in a narrative format. In reality, fraud is very different than money laundering. Fraud prevention is reactive and urgent rather than retrospective. Fraud and scam signals are more time sensitive, with immediate action and decisioning to effectively prevent fraud and scams. Additionally, the signals are better consumed as specific data elements related to application, digital fingerprints, login data, and transaction initiation. To prevent and investigate fraud and scams, a more modern fraud-specific reporting system that captures data in a consistent manner would allow the data gathered to be more immediately actioned and potentially shared to prevent fraud and lead to more meaningful fraud investigations. Transitioning fraud from the Suspicious Activity Reporting process to a modern Fraud Signal Report would lead to more valuable and actionable data gathering by the government.

This sort of information-sharing effort could be further strengthened through the creation of a centralized fraud database to identify fraud signals, patterns of conduct, and repeat bad actors to leverage for fraud prevention. These initiatives should be supported by a proactive risk management approach that anticipates emerging threats through advanced analytics, consortium data, vendor partnerships, and real-time alerts paired with customer verification protocols.

According to an October 2025 study by researchers from Notre Dame and Carnegie Mellon universities, the number one thing a bank can do to retain a customer after a fraud incident is to identify the perpetrator.[22]

This underscores that victims want accountability and to deliver it, industry and government must share information more effectively, investigate more efficiently, and remove the operational and legal barriers that keep us from tracking down and stopping bad actors.

Education Including a Nationally Coordinated Fraud and Scam Awareness Campaign

Education is equally vital and must continually evolve to meet the challenges posed by increasingly sophisticated fraud schemes. Bank-led education efforts are most effective when delivered at key touchpoints, such as onboarding, product discussions, and annual reviews, using direct prompts that require user acknowledgment. These measures introduce thoughtful friction, creating meaningful pauses that encourage consumers to reassess potential risks. Real-time, personalized guidance from trusted banking professionals remains effective – though less scalable – method, particularly in countering rapidly shifting tactics and misleading social narratives that minimize the harm of scams.

Industry-wide collaboration is also critical. Partners benefit from specialized, ongoing education that emphasizes a holistic, end-to-end view of the fraud and scam lifecycle. A broad, nationally coordinated fraud and scam awareness campaign, similar in scale and visibility to Smokey Bear's wildfire prevention initiative, could help reach diverse audiences and shift public perception. The United Kingdom has shown this could be successful with their "Take Five to Stop Fraud" campaign. The shared challenge is connecting consumers with the necessary tools and knowledge *before* they become victims, which requires sustained innovation, cross-sector coordination, and a comprehensive understanding of fraud's lifecycle. New solutions and partnerships are especially important as a growing share of financial crimes originates overseas through organized global networks.

Expanding Fraud Mitigation Services at the Federal Reserve System

Operationally, expanding fraud mitigation services within the Federal Reserve System and developing centralized tools to support law enforcement in tracking and sharing fraud data would help prevent harm before it occurs and ensure that fraudsters are identified, apprehended, and prosecuted before they can victimize additional consumers.

---

[22] https://mendoza.nd.edu/news/banks-that-identify-fraudsters-increase-loyalty/

At the same time, anti-fraud tools and regulatory frameworks must be modernized to keep pace with increasingly sophisticated threats. For example, modernizing Regulation CC could significantly reduce consumers' exposure to fraud. Consumer protections would be strengthened by clarifying that, although certain Regulation CC exceptions may not apply to electronic payments, other fraud-related and anti-money laundering obligations may supersede next-day availability requirements. Providing greater flexibility under Regulation CC to implement enhanced check fraud safeguards – such as expanding exception holds based on fraud risk and broadening the definition and scope of "new account" exception holds – would support continued investment in modern payment systems while maintaining appropriate consumer protections. Additionally, timelines for submitting, handling, and responding to claims should reflect the modern reality that investigations often rely on instantaneously shared images rather than physically transported documents.

Conclusion

The fraud and scam epidemic confronting American consumers is not a series of isolated incidents. It is a rapidly evolving, technology-accelerated, globally coordinated threat that inflicts billions of dollars in losses each year and undermines trust in reputable institutions. Banks like EverBank are investing heavily in people, technology, education, and partnerships to protect our customers, but we cannot win this fight alone. The fact of the matter is that fraud today does not begin at the bank, and it cannot be solved by banks alone.

A whole-of-government strategy that brings together financial regulators, law enforcement, technology companies, telecommunications providers, and social media companies to address the root causes of fraud and scams before they reach our customers is critically necessary.

The good news is that this Committee, and Congress as a whole, have the opportunity to take important steps to further empower the public and private sector to combat the growing fraud and scam epidemic.

EverBank, and the Consumer Bankers Association's membership more broadly remain committed to working with you to increase public and private sector coordination, better protect consumers, and address the root causes of fraud and scams.

Thank you for your attention and for your leadership on this critical issue. I look forward to your questions.

Chairman BARR. Thank you.

Ms. McKune, you are now recognized for 5 minutes.

STATEMENT OF KATE McKUNE, GENERAL COUNSEL, PARK COMMUNITY CREDIT UNION, ON BEHALF OF AMERICA'S CREDIT UNIONS (ACU)

Ms. MCKUNE. Good morning, Chairman Barr, Ranking Member Foster, and members of the subcommittee.

I am Kate McKune, general counsel of Park Community Credit Union in Louisville, Kentucky. I am pleased to appear before you today on behalf of America's Credit Unions, where I serve on the Fraud Task Force and the association's Advocacy Policy Committee.

We applaud the subcommittee for holding this important hearing today.

Financial institutions operate in an environment where fraud and scams are becoming increasingly more prevalent.

Fraud encompasses a wide range of criminal tactics. Scams, as a subset of fraud, often involve an element of impersonation or trickery.

Both ultimately harm the consumer and the financial institution and fall under the broader scope of fraud being examined at this hearing today.

Credit unions like mine must contend with a fraud environment where a large share of fraud and scams originate outside of the financial sector, and criminal sophistication continues to grow.

Credit unions are the original consumer protectors, and that fact puts us at the forefront of looking out for our members.

At the same time, consumers increasingly demand speed and convenience as a core part of their banking experience.

Sometimes the only viable defense against fraud is preventing it before it occurs, a process that can be technologically demanding, expensive, and dependent on timely information sharing between law enforcement, Federal regulators, and other payment system stakeholders.

Despite significant investments in fraud detection tools, consumer education, and data security, credit unions report each year that fraud remains a top concern.

For smaller credit unions, a significant fraud loss could impact the financial health of the institution.

As a not-for-profit cooperative, if regulatory standards on liability for fraud were to shift the costs further to the institution, our members would ultimately bear the burden.

Credit unions regularly work to adapt, innovate, and educate their members about the variety of fraud and different scams that can target them—although, oftentimes, no amount of security investment or intervention can fully compensate for a consumer's decision to trust a scammer.

One of the biggest challenges in combating fraud is that it can come in so many different forms.

Romance scams can be difficult for a credit union to detect and prevent because manipulation of the victim can take place over a long period of time. Often, victims of romance scams will genuinely

believe that their online friend is a person they can trust, and no amount of circumstantial evidence will change their mind.

Fraudulent advertisements for fake goods and services are another common vector for defrauding consumers.

Unfortunately, financial institutions have minimal control over how online or social media entities manage their advertising policies. As a result, we must resort to simply warning consumers that completely anonymous, online, sight-unseen purchases of goods could mean losing their money.

Investment scams and business impersonation scams have also contributed to abnormally high fraud losses among consumers. Often, these scams can involve cryptocurrencies or impersonators pretending to work for crypto companies.

Check fraud has also increased in recent years. One way to combat this would be to modernize the funds availability rules under Regulation CC and create flexibility in the length of time funds may be held if there are concerns about a check.

While the National Credit Union Administration (NCUA) also provides resources to assist credit unions and their members in the fight against fraud, America's Credit Unions supports greater interagency coordination, expanded information-sharing authority, and close collaboration with law enforcement to address fraud.

We believe a national strategy to mitigate fraud should include several key elements.

First, improving information sharing and coordination. Bills such as the TRAPS Act and TRACE Act are important steps in this area that would improve cooperation between public and private sectors and law enforcement.

Second, a national consumer education campaign and program from the Federal Government that partners with industry.

Third, modernization of funds availability rules. Legislation such as the STOP Fraud Act would begin to make improvements in this area.

Fourth, promotion of the use of technology, including AI, to help combat fraud. The Bank Fraud Technology Advancement Act is an important first step. We also support the creation of technical assistance and grant programs to help smaller financial institutions access best-in-class technology.

In conclusion, there is no magic bullet to stop fraud and scams. At Park Community, we are on the front lines trying to fight it and help our members, but the challenges are complex. Often, criminals seek to manipulate the system and prey on human nature.

There is only so much one institution can do alone. What is needed is a commitment at the Federal level to work with credit unions and other financial institutions to help combat fraud and scams by using an all-of-government approach as outlined in my testimony.

Thank you for holding this important hearing and for the opportunity to appear before you today. I welcome any questions you may have.

[The prepared statement of Ms. McKune follows:]

America's Credit Unions

Testimony of

Kate McKune
General Counsel & Vice President Enterprise Risk
Park Community Credit Union
on behalf of
America's Credit Unions

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

Before the
Subcommittee on Financial Institutions
House Committee on Financial Services

March 5, 2026

Introduction

Good morning, Chairman Barr, Ranking Member Foster, and Members of the Subcommittee. I am Kate McKune, General Counsel at Park Community Credit Union in Louisville, Kentucky. I am pleased to appear before you today on behalf of America's Credit Unions where I serve on the Fraud Task Force and the association's Advocacy Policy Committee. I joined Park Community in 2017 after 15 years working as an attorney in commercial litigation practice. At the credit union I established the legal department and have overseen various areas, including compliance, risk, fraud, internal audit, and our institution's insurance program.

About Park Community Credit Union

Park Community was founded in 1965 in Louisville by the GE Appliance employees at Appliance Park to provide low-cost loans to one another, when they had been shut out of more traditional sources of credit. As the credit union grew, we eventually became community chartered and then ultimately a multiple-common bond federal credit union in 2021. Today we are a Low-Income Designated credit union with branches in the greater Lexington and Louisville metropolitan areas, including two in the southern Indiana suburbs. We have about 80,000 members and $1.4 billion in assets. We are also recognized as a Community Development Financial Institution (CDFI) with over 70 percent of our loans (both by number and assets) going to CDFI members.

Background on Credit Unions

Credit unions serve a unique function in the delivery of necessary financial services to Americans. Credit unions are the original consumer financial protectors because of our not-for-profit, member-owned cooperative structure that aligns the interest of the credit union with its members. Member-ownership and not-for-profit status results in a wide range of pro-consumer credit union behaviors. Credit union members across the country recognize the real measurable "transformative power" associated with cooperative finance.

Every credit union is a cooperative institution organized "for the purpose of promoting thrift among its members and creating a source of credit for provident or productive

purposes" (12 § USC 1752(1)). Congress established the federal credit union system to meet a precise public need—and today credit unions provide financial services to over 145 million Americans. Since President Franklin D. Roosevelt signed the Federal Credit Union Act (FCU Act) into law more than 91 years ago, two fundamental principles regarding the operation of credit unions remain every bit as important today as in 1934:

1. Credit unions remain totally committed to providing their members with efficient, low-cost, personal financial services; and
2. Credit unions continue to emphasize traditional cooperative values such as democracy and volunteerism.

The nation's approximately 4,500 credit unions serve a different purpose and have a fundamentally different structure than many other financial institutions. Credit unions exist solely for providing financial services to their members. As owners of cooperative financial institutions, united by a common bond, all credit union members have an equal say in the operation of their credit union—"one member, one vote"—regardless of the dollar amount they have on account. These singular rights extend all the way from making basic operating decisions to electing the generally unpaid, volunteer board of directors. Credit unions continue to play a very important role in the lives of millions of Americans from all walks of life. Since the Great Recession, consolidation of the financial institution sector has progressed at an increasingly rapid rate. Credit unions are second-to-none in providing their members with quality personal financial services at the lowest possible cost.

The Challenge of Preventing Fraud

We applaud the Subcommittee for holding this important hearing today. Financial institutions operate in an environment where fraud and scams are becoming increasingly more prevalent. "Fraud" and "scams" are technically different: "fraud" is generally when the criminal steals a victim's money without their knowledge and a "scam" generally tricks them to turn over money or credentials by dishonest means. Both ultimately harm the consumer and the financial institution and fall under the broader scope of fraud being examined at this hearing today.

Credit unions like mine must contend with a fraud environment where a large share of fraud and scams originate outside of the financial sector and criminal sophistication continues to grow. At the same time, consumers increasingly demand speed and convenience as a core part of their banking experience. Sometimes the only viable defense against fraud is preventing it before it occurs, a process that can be technologically demanding, expensive, and dependent on timely information sharing between law enforcement, federal regulators, and other payment system stakeholders. In some cases, preventing fraud before it occurs is nearly impossible due to the nature of certain payment instruments—like checks—which can easily be stolen, altered, or forged.

Despite significant investments in fraud detection tools, consumer education, and data security, credit unions report each year that fraud remains a top concern. For smaller credit unions, where the risk of a significant fraud loss could impact the financial health of the institution, there is a sense that if regulatory standards on liability for fraud were to shift further to the institution, it would be difficult to manage the monetary costs of providing basic banking services like debit cards or credit cards—particularly in an environment where Congress may be considering further reductions in or limiting of interchange rates which play an important role in helping protect a consumer's data over card networks.

It is no different at Park Community. Like all credit unions, we train staff, formally and informally, to prevent elder abuse on a consistent basis. All branch and ITM staff complete fraud training sessions that cover common types of check fraud/scams and provide examples of real fraudulent checks that were presented at Park Community to talk through as a group. They also complete a course that provides knowledge on regulations, guidelines, and best practices related to fraud prevention on negotiable instruments. We also assign Elder Financial Abuse - Awareness and Prevention to all Park Community staff on an annual basis, which includes information on detecting when our members are being financially abused or exploited.

We also empower staff to slow down and ask for help if they suspect a member is being scammed. We have internal processes to capture Incident Reports of Suspicious Activity, and we work with local programs to protect vulnerable seniors. We also train staff to understand that anyone can be a victim of a scam or fraud, no matter their age. Even with all of these efforts, fraud is still a fact of life at a financial institution like mine.

While our fraud loss prevention efforts are successful and at an all-time high (over $1 million prevented in 2025), our charge-offs from fraud are also up (over $300,000 in both 2024 and 2025) as the volume of fraud we face is increasing. We had nearly 6,500 fraud alerts in 2025, which averages to nearly 20 a day.

Types of Scams Impacting Credit Union Members

Total U.S. industry reports indicate that fraud losses totaled $132 billion in 2023, and the Federal Trade Commission (FTC) has published data indicating that scams alone cost American consumers $12.5 billion in 2024.[1] The Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3) has also reported that cyber-related crime contributed to a record $16.6 billion in losses in 2024 and fraud contributed to the bulk of the losses.

One of the biggest challenges in combatting fraud is that it can come in so many different forms. Closing one door, or stopping one form, is likely only to increase another. These forms are also constantly changing and expanding, which presents a challenge to a community financial institution like mine, as we need to constantly adapt, innovate, and educate.

Credit unions are working to educate their members about a variety of different scams that can target them, which are varied in their tactics but are generally alike insofar as they prey upon weaknesses in human judgment. Oftentimes, no amount of security

[1] *See* Nasdaq – Verafin, 2024 Global Financial Crime Report; FTC, "New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024" (March 10, 2025), *available at* https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024.

investment or lawful intervention can fully compensate for a consumer's decision to trust a scammer. According to the FTC, imposter scams—which include things like romance scams and tech support scams—are the most common category of fraud reported by consumers since July 1, 2023.[2] According to the FTC, imposter scams cost American consumers $3 billion in reported losses in 2024. Some of the most common scams we see include:

- Romance scams. Romance scams can be difficult for a credit union to detect and prevent because manipulation of the victim can take place over a long period of time. Often victims of romance scams will genuinely believe that their online "friend" is a person they can trust and no amount of circumstantial evidence will change their mind. These scams are also challenging to mitigate because they originate on platforms that are not visible to financial institutions or federal regulators. At Park Community we had a recent example where one of our members was targeted in one of these scams where the fraudster spent *two years* establishing an online relationship before asking for money. This just shows the depth and patience of these scammers. While the FTC can pursue enforcement actions against online companies that deceive or abuse consumers, the FTC does not always have the requisite supervisory authority to intervene and demand mitigating action before harm occurs.

- Tech support and business impersonation scams. According to the FTC, in 2024, consumers 60 and older were five times more likely than younger people to report losing money on a tech support scam. Older consumers reported $159 million in losses to tech support scams in 2024.[3] FTC data indicates that the toll of business impersonation scams is even greater, with consumers losing a combined $2.95 billion in 2024.[4] Oftentimes these scams propagate through spoofed phone calls or

[2] *See* FTC, The FTC's Efforts in the Greater Fight Against Ransomware and Cyber-Related Attacks, 27 (2025), *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/p035303ransomwarereport2025.pdf.
[3] *See* FTC, Protecting Older Consumers 2024-2025, 13 (December 1, 2025), *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/P144400-OlderAdultsReportDec2025.pdf.
[4] *See* FTC, FTC Highlights Actions to Protect Consumers from Impersonation Scams (April 4, 2025), *available at* https://www.ftc.gov/news-events/news/press-releases/2025/04/ftc-highlights-actions-protect-consumers-impersonation-scams

text messages. While private solutions exist for businesses to verify their caller ID, vendor branding can be costly and does not address the present threat of criminals receiving A-level attestations from voice service providers when placing spoofed calls.[5] These challenges illustrate the need for a strong, cross-sector approach to addressing fraud and close collaboration between financial regulators, law enforcement, and the Federal Communications Commission (FCC).

- Fraudulent advertisements. Fraudulent advertisements for fake or misleading goods and services are another common vector for defrauding consumers. Unfortunately, financial institutions have minimal control over how online marketplaces, forums, or social media manage their advertising policies. As a result, credit unions must resort to simply warning consumers that completely anonymous, online, sight-unseen purchases of goods could mean losing your money. Legislation such as H.R. 7548, the Safeguarding Consumers from Advertising Misconduct (SCAM) Act, would help to address this issue by asking social media companies to remove scammers from their platforms.

- Investment scams. The FBI and FTC have noted a surge in investments scams, which have contributed to abnormally high fraud losses among consumers. Often these scams involve cryptocurrencies, highlighting the need for clarification regarding the responsibilities of parties involved in digital asset transactions.[6] Often these scams involve impersonators pretending to work for call centers at cryptocurrency exchanges.[7] According to the FTC, investment scams were the number one way that consumers were defrauded in 2024.

---

[5] *See* Joint Trades Letter In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls, CG Docket No. 17-59, (January 5, 2026), *available at* https://americascus.widen.net/view/pdf/aad4aad8-7b7a-49fc-bc43-d357ec2826b9/JointclTCPA20260105.pdf.
[6] *See* FTC, "New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024" (March 10, 2025), *available at* https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024.
[7] *Supra* note 2 at 11.

No matter what type of scam is involved, credit unions are committed to protecting their members from criminals. The National Credit Union Administration (NCUA) also provides resources to assist credit unions and credit union members in the fight against fraud. The NCUA hosts a variety of resources on MyCreditUnion.gov to educate members about common types of scams, identity theft, cyber threats, and how to report suspected fraud.[8] The NCUA has also provided credit unions with risk alerts concerning different types of criminal tactics used to defraud members or compromise credit union systems.[9]

Notwithstanding the abundance of consumer resources that both credit unions and the NCUA provide to help credit unions protect themselves, there is, perhaps, a misperception that to achieve meaningful consumer protection regulators must somehow balance incentives and penalties as if there were no intrinsic motivation to fight fraud. The reality is that credit unions are voluntarily doing everything they can to protect their members' funds because the financial health of the credit union is synonymous with the financial health of its members. As financial cooperatives that do not issue stock, any loss of a member's funds is a loss of the credit union's paid-in and unimpaired capital and surplus.[10] It is this same principle that makes it unfair to simply shift the liability of fraud perpetrated against a member onto the credit union, for both individual members and the credit union as an institution. This cost of being responsible for the actions of others, when reasonable steps were taken to try to help the member and prevent the scam, can have a significant negative impact on the credit union. Transferring liability for a wider range of fraudulent transactions would invite de-risking strategies that could ultimately harm consumer access to banking services, embolden criminals, and signal to consumers that there is no penalty for lack of caution in their own financial affairs. That is why we oppose efforts to shift liability to financial institutions under Regulation E.

---

[8] *See* NCUA, https://mycreditunion.gov/protect-your-money/prevention/frauds-scams.
[9] *See e.g.*, NCUA, Risk Alert, Business Email Compromise through Exploitation of Cloud-Based Email Services, 21-RISK-01 (October 2021).
[10] 12 USC § 1795a(2) ("'paid-in and unimpaired capital and surplus' means the balance of the paid-in share accounts and deposits as of a given date, less any loss that may have been incurred for which there is no reserve or which has not been charged against undivided earnings, plus the credit balance (or less the debit balance) of the undivided earnings account as of a given date, after all losses have been provided for and net earnings or net losses have been added thereto or deducted therefrom.").

Credit unions want their members to be protected. Often local law enforcement does not have the resources, nor the jurisdiction, to address many of the fraud and scams they face. That is why additional efforts to combat scams, as outlined later in my testimony, are ultimately needed at the federal level.

Check Fraud

Another major type of fraud impacting financial institutions is check fraud. Credit unions report that check fraud has increased in recent years. Reports from the U.S. Postal Inspection Service indicate that the U.S. Postal Service (USPS) recovers over $1 billion in counterfeit checks and money orders each year. Other USPS reports have drawn attention to checks being stolen out of mailboxes, including the theft of U.S. Treasury checks which are generally granted near-immediate, next-day funds availability when deposited.

Check washing schemes (i.e., alteration by chemical process) and use of counterfeit cashier's checks or Treasury checks (privileged categories of checks which grant consumers faster access to funds) have long been a concern. In February 2023, the Financial Crimes Enforcement Network (FinCEN) released an alert warning financial institutions of "a nationwide surge in mail theft-related check fraud schemes." In the alert, FinCEN noted that Bank Secrecy Act (BSA) reporting for check fraud had increased over the past three years. Between 2020 and 2021, FinCEN observed a 23 percent increase in the number of check fraud-related Suspicious Activity Reports (SARs) filed by financial institutions.

We commend the U.S. Department of the Treasury's efforts to modernize federal payment systems to reduce fraud. Executive Oder 14247, titled "Modernizing Payments To and From America's Bank Account," has helped promote secure electronic payments of government funds and reduce the risk of financial institutions mistakenly paying fraudulent government checks.

Still, more can be done to reform regulations governing the handling of checks to improve financial institutions' defense against check fraud that involves non-government checks. For example, modernizing funds availability rules under Regulation CC could address

fraud that exploits the idiosyncrasies of check processing and regulatory limits on hold times.

Financial institutions would benefit from a more flexible interpretation of Regulation CC's reasonable cause to doubt the collectibility exception. There are two components to this exception which the Federal Reserve and the Consumer Financial Protection Bureau (CFPB) should consider, since both agencies currently have overlapping authority to administer the rule.

The first component relates to the reasons for doubting an item's collectiblity, which can be numerous and complex. Documenting in detail a financial institution's reason for believing that a check is uncollectible, as required by the rule, can pose great challenges. Credit unions report difficulty in scaling systems when attempting to articulate and explain meaningful and understandable reasons for invoking a particular exception to delay funds availability—a difficulty that reflects the fact that checks are often processed using systems with multiple data points that are subject to complex multi-factored analysis. Explaining the finer points of such analysis to comply with notice requirements could reveal proprietary fraud detection methods to criminals and inadvertently lead to the development of new evasion tactics.

The second component that should be addressed in Regulation CC relates to the length of time that funds may be held, which is defined in the Expedited Funds Availability Act (EFA Act) as a "reasonable period," a term that is subject to regulatory interpretation. More flexibility regarding the length of extended holds (i.e., the reasonable period) that applies to checks under this exception would be helpful in investigating fraud. Five business days is often insufficient time to determine the collectibility of a check. The Federal Reserve has not attempted to conduct a representative survey of the sufficiency of existing hold times under Regulation CC since its Report to Congress on the Check Clearing for the 21st Century Act of 2003. We believe legislation that consolidates within a single agency the responsibility for administering Regulation CC would greatly accelerate regulatory reform efforts.

Even outside the domain of checks, additional speed bumps, or the ability to hold electronically deposited funds to investigate fraud when there is reasonable suspicion, would greatly aid efforts to defeat criminal tactics. At the heart of many scams is a false sense of urgency—the criminal's insistence that the consumer must act immediately, without reflection. Consequently, payment speed is a benefit to both consumers and criminals depending on the context. But it may be worthwhile for regulators to consider whether expeditious settlement should be guaranteed as a legal right given the magnitude of fraud today.

Legislative Actions that Would Help Combat Growing Fraud Losses

America's Credit Unions supports greater interagency coordination, expanded information sharing authority, and close collaboration with law enforcement to address fraud. An effective national strategy to mitigate fraud should also prioritize the following objectives:

1. Encourage the use of innovative technology, including artificial intelligence, to improve early warning capabilities;
2. Offer technical assistance and grants to support efficient information exchange between small, community financial institutions and other payment system stakeholders;
3. Promote regulatory modernization (particularly for funds availability rules); and,
4. Prioritize consumer education.

I expand on a number of these and other concepts below.

Need for improved stakeholder coordination. Financial regulators should recognize that financial institutions are often limited in their ability to target the root causes of fraud. Criminals can easily adopt new tactics that prey on vulnerabilities present in less regulated parts of the economy, such as online marketplaces. Accordingly, a whole-of-government approach is necessary to effectively combat payments fraud in all its forms, and agencies like the FCC, FTC and Department of Justice (DOJ) should join the work of

the federal financial regulators, under the leadership of the Treasury Department, to determine what actions can be taken to stop impersonators and other scammers.

We are extremely supportive and appreciative of the Administration's efforts to direct interagency efforts towards combatting fraud. We could also support additional Executive Orders to bring about a wider whole-of-government approach.

Strengthening collaboration among financial institutions, law enforcement, and regulatory bodies is also of paramount importance. Opportunities for improvement include:

- Establishing local and regional fraud task forces to coordinate investigation and recovery efforts and share intelligence.
- Establishing dedicated financial sector liaisons within regional federal law enforcement offices to promote intelligence exchange with industry partners.
- Encouraging membership in organizations like the International Association of Financial Crimes Investigators (IAFCI) to foster industry-wide collaboration.
- Creating secure platforms for FI-to-FI exchange information, including scam data, while protecting personally-identifiable information.
- Expanding and encouraging full participation in the 314(b) Program.
- Encouraging more willingness on the part of financial institutions to report payment fraud to law enforcement authorities, and more willingness on the part of those authorities to take and share responsive action.

We are also strongly supportive of H.R. 4936, the Taskforce for Recognizing and Averting Payment Scams (TRAPS) Act, which takes important steps to bring industry, including credit unions, together with regulators to work to develop ways to combat scams. We urge the Committee to advance this bill as soon as possible.

Support information sharing efforts. The collection and centralized sharing of fraud-related information would aid efforts to develop better tools designed to stop suspicious

transactions before they occur. While credit unions already file SARs with FinCEN, access to this information is generally limited. Section 314(b) of the USA PATRIOT Act currently provides financial institutions with the ability to share information under a safe harbor that offers protections from liability. The information sharing safe harbor created by Section 314(b) is limited to reports of unlawful transactions involving money laundering or terrorist financing—not general fraud, which could encompass things like mortgage application fraud or payments fraud. Given uncertainty about the scope of the safe harbor under Section 314(b) when a transaction does not clearly involve money laundering or terrorist financing, maximizing the scope of permissible information sharing to target general financial fraud could enhance existing information sharing efforts. We could support efforts to expand this safe harbor to include fraud.

While expanded legal authority is important, smaller financial institutions may also face the challenge of having limited resources to engage in robust information sharing activities that depend on peer communication. At small credit unions in particular, the number of employees equipped to handle external inquiries related to particular transactions is highly limited, and resources are often already stretched thin. Technical assistance and grants to support greater information exchange could help alleviate the problem of limited resources and employee bandwidth. Creation of a new grant program, expansion of the NCUA's current Community Development Revolving Loan Fund, or even the CDFI Fund are all potential options.

At the same time, Congress should be cautious about inadvertently expanding BSA/anti-money laundering (AML) reporting obligations in conjunction with greater reporting flexibility. The current SAR forms are ultimately retrospective and not prospective. An institution's resources may be better utilized to combat fraud if reporting requirements were modernized, including raised reporting thresholds such as proposed in H.R. 1799, the Financial Reporting Threshold Modernization Act, which America's Credit Unions supports.

To minimize operational disruption, enhanced information sharing authorities should aim to facilitate *voluntary* exchange between financial institutions and not establish new burdens that ultimately drain resources from the front lines of fighting fraud.

Ultimately, for credit unions to have confidence in expanded information sharing authorities, there must be a commensurate focus on providing adequate legal safe harbors and appropriate limitations on liability.

Encourage use of innovative technology. Emerging technologies (such as AI and biometrics) can play a significant role in preventing fraud. Congress and federal banking agencies should aim to ease adoption of these new technologies rather than create supervisory friction.

Innovative technology is also necessary to keep pace with state-of-the-art fraud tactics which are becoming cheaper and easier to access. For example, generative AI has made impersonation scams particularly dangerous, with criminals now having access to tools that can cheaply recreate a person's voice and appearance. Credit unions should have the flexibility to adopt countermeasures that may be imperfect, but better than nothing, rather than face supervisory scrutiny if a solution does not execute perfectly.

Promote regulatory modernization. Legal complexities and liability currently surrounding data sharing could be reduced by 1) implementing a safe harbor framework to protect financial institutions when sharing sensitive data to combat fraud, and 2) standardizing information sharing protocols, allowing for increased visibility of data across financial institutions.

We also believe that Congress should also consider modernizing the EFA Act to provide financial institutions with greater flexibility to hold deposited funds when there is suspected financial fraud. Many states have successfully adopted legislation that balances consumer privacy and access to funds with the broader interest in preventing consumer harm and criminal activity.

Trusted contacts.: Some states have established trusted contact laws to help those who may be the most vulnerable to scams. Allowing an institution the discretion to verify with a pre-determined trusted contact on questionable transactions could be a solution. However, it is important that this approach not become overly prescriptive, as it is not foolproof and can delay legitimate transactions and place potential time-consuming burdens on the institution.

Consumer education. Consumer education is a foundational element of an effective anti-fraud strategy. Credit unions report that where a member has fallen victim to a payment fraud scam, the ideal response is to provide outreach on an individual basis with examples of how to recognize and avoid similar situations in the future. Consumers who are victims of fraud sometimes report that shame or embarrassment prevents them from reaching out to their financial institution to ask what they might have done differently to prevent loss of funds. Consumer education should be presented in a way that helps to overcome this stigma.

Credit unions often provide resources and tips for avoiding future payment fraud scams. However, such personalized education is not scalable and typically occurs after the member has already fallen for a scam. Many financial institutions have explored just-in-time intervention, such as push notifications, to alert members of suspicious account or transaction activity; however, these systems are not a substitute for sound judgement and the exercise of caution.

Increased and sustained public messaging from trusted sources involving multiple media channels would be useful in educating consumers on how to better protect themselves from payment fraud scams. A dedication of resources and commitment to a large national campaign by government agencies, in partnership with industry, to educate consumers on scams and fraud is one potential option to help address this.

Legislation Noticed for this Hearing

America's Credit Unions is generally supportive of the discussion drafts noticed for this hearing as we believe they take key steps to addressing the issues outlined in my testimony above:

The "Transaction Risk Analytics and Collaborative Exchange (TRACE) Act of 2026": This will take important steps to allow financial institutions to share information in efforts to combat fraud. As noted in my testimony above, we could also support expanding this legislation to amend Section 314(b) of the USA PATRIOT Act to include fraud.

The "Scrutinizing Transactions for Overt Payment (STOP) Fraud Act of 2026": This draft bill addresses issues outlined in my testimony above by allowing financial institutions to better scrutinize Treasury and cashier's checks, as well as fraudulent wire transfers and electronic transactions.

The "Bank Fraud Technology Advancement Act of 2026": This legislation would require financial regulators and law enforcement to study and report to Congress on how technology can be better used to combat scams and fraud. This is an important step as I have noted in my testimony above.

Conclusion

Credit unions like Park Community and our members are under constant attack from criminals that seek to perpetrate fraud and scams. At Park Community we are on the front lines trying to fight it and help our members, but the challenges are complex. Often these criminals seek to manipulate the system and prey on human nature. There is only so much we can do as an institution, and concentrating the cost of the frailties of human nature on the financial institution is not the answer.

What is needed is a commitment at the federal level to work with financial institutions to help combat fraud and scams by using an all-of-government approach. Key elements of this include avenues and protections for increased information sharing, modernizing of regulations and elimination of onerous regulatory burdens, the ability to use technology

in the fight against fraud and scams, and a national consumer education effort to heighten awareness.

Unfortunately, there is no magic bullet to stop fraud and scams. Regulatory and legislative solutions like those approaches noticed for this hearing, and others including, but not limited to, the TRAPS Act are needed.

Thank you for holding this important hearing and the opportunity to appear before you today. I welcome any questions you may have.

Chairman BARR. Thank you.

Mr. Schuster, you are now recognized for 5 minutes.

STATEMENT OF JOSEPH J. SCHUSTER, PARTNER, BALLARD SPAHR LLP

Mr. SCHUSTER. Thank you, and good morning. Chairman Barr, Ranking Member Foster, and members of the subcommittee, thank you for the opportunity to testify today.

My name is Joseph Schuster, and I am a partner in Ballard Spahr's Consumer Financial Services Group, where I advise banks, credit unions, payment companies, and technology providers on Federal and State consumer finance laws.

A substantial portion of my practice focuses on fraud-and scam-related matters, including payment fraud, identity-based fraud, account takeover, check and wire fraud, scam typologies, loss allocation, and legal and operational frameworks governing fraud detection and response.

Throughout my testimony, two themes are going to be pervasive. The first is the challenge of sharing information effectively to prevent fraud. The second is the constraints financial institutions face when deploying new tools to combat rapidly evolving fraud schemes.

Fraud prevention today is inherently collaborative. It depends on coordination among financial institutions, their service providers, law enforcement, and in many cases cross-industry information-sharing networks. Yet, these efforts take place within a layered legal and supervisory framework.

Fraud mitigation is shaped not only by statutory regimes, such as the Fair Credit Reporting Act and the Expedited Funds Availability Act, but also by regulatory guidance, supervisory expectations, and the practical realities of examinations and investigative oversight.

Financial institutions must navigate Federal and State compliance expectations and requirements while simultaneously responding to increasingly sophisticated and fast-moving fraud threats.

The interaction between Federal and State law can create uncertainty in areas such as information sharing, funds availability practices, fraud-related holds, consumer dispute handling, and the use of advanced analytics.

Institutions operating nationally must reconcile these overlapping regimes while responding to fraud schemes that do not respect jurisdictional boundaries.

My testimony today reflects a legal practitioner's perspective across institutions of varying sizes and business models.

Fraud has evolved rapidly in recent years. At the same time, many elements of the legal and supervisory framework were developed in an era when fraud was slower, more siloed, and certainly less technologically advanced.

The result is a growing tension between the speed and scale of emerging fraud trends and the structure of the regulatory architecture governing prevention efforts.

I appreciate the committee's attention to these issues, and I look forward to discussing how policymakers can support effective fraud

mitigation while preserving consumer protections, privacy, and fair access to financial services.

Thank you.

[The prepared statement of Mr. Schuster follows:]

Written Testimony before the House Financial Services Committee
Subcommittee on Financial Institutions

Joseph J. Schuster
Partner
Ballard Spahr LLP

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

March 5, 2026

Table of Contents

Page

I. Introduction 1
II. Emerging Fraud Trends Affecting Financial Institutions 2
a. Check Fraud 2
b. Social Engineering: Fraudulent Inducement at Scale 3
c. Fraud in Faster Payments and Cross-Rail Exploitation 4
d. Identity-Centric Fraud: Synthetic Identity and Credential Abuse 6
III. The Challenges Financial Institutions are Facing with Emerging Fraud Trends 6
a. Balancing Fraud Prevention with Customer Experience and Access 6
b. Operating in Real Time with Compressed Decision Windows 8
c. Information Silos and Fragmented Visibility 8
d. Legal and Supervisory Uncertainty 9
e. Technology Deployment and Governance Complexity 10
f. Resource Constraints for Community Institutions 10
IV. Legal and Regulatory Framework Governing Fraud Prevention 11
a. Statutes 11
b. Regulatory Guidance 13
c. Supervisory Expectations 13
d. State Laws 14
V. Areas Where Current Law Constrains Fraud Prevention Efforts 15
a. Constraints on Information Sharing and Collaborative Fraud Mitigation 15
b. Funds Availability and the Operational Reality of Modern Check Fraud 16
c. Supervisory and UDAAP Risk That Can Discourage Proactive Intervention 16
d. Liability Allocation Challenges in Multi-Platform Fraud Environments 17
e. State Privacy and Emerging State AI Laws Create Additional Friction for Modern Fraud Technology 18
VI. Opportunities for Policymakers to Support Fraud Prevention 19
a. Establish a Fraud-Prevention Safe Harbor Under the FCRA 19
b. Clarify and Expand Section 314(b) for Fraud Coordination 19
c. Provide Safe Harbors for Risk-Based Fraud Controls Under ECOA and TILA 20
d. Establish a Dynamic Commercially Reasonable Security Safe Harbor 21
e. Direction to Regulators 21
VII. Conclusion 24

I. Introduction

Chairman Hill, Ranking Member Waters, and Members of the Committee:
Thank you for the opportunity to testify at today's hearing, *Fighting Fraud on the Front Lines: Challenges and Opportunities for Financial Institutions*.

I am a partner in Ballard Spahr LLP's Consumer Financial Services Group, where I advise banks, credit unions, payments companies, and technology providers that support financial institutions on federal and state consumer financial laws. A substantial portion of my practice is devoted to fraud-related matters, including payments fraud, identity-based fraud, account takeover, check and wire fraud, scam typologies, loss allocation, and the operational and legal frameworks governing fraud detection and response. I previously served as a Managing Director and Senior Counsel at Goldman Sachs Bank USA, which provided me with direct, in-house experience navigating the practical and operational realities financial institutions face in complying with the legal frameworks discussed today.

I regularly work not only with financial institutions themselves, but also with the technology companies that design and deploy fraud detection systems, identity verification tools, behavioral analytics, and information-sharing utilities. Fraud prevention today is a coordinated effort that depends on financial institutions, their service providers, and inter-institution collaboration.

These efforts take place within a layered legal and supervisory framework. Fraud prevention is shaped not only by statutory regimes, such as the Electronic Fund Transfer Act, Truth in Lending Act, Fair Credit Reporting Act, Expedited Funds Availability Act, Gramm-Leach-Bliley Act, and the Bank Secrecy Act, but also by regulatory guidance, supervisory expectations, and the practical realities of examinations and investigative oversight. Financial institutions must navigate compliance reviews, model risk expectations, fair lending considerations, UDAAP standards, vendor oversight, and cybersecurity requirements while simultaneously responding to increasingly sophisticated and fast-moving fraud threats.

In addition, financial institutions must navigate state consumer protection statutes, state privacy, data usage, and artificial intelligence laws, and state-level enforcement authorities, which may impose additional or overlapping requirements. The interaction between federal and state law can create uncertainty in areas such as information sharing, funds availability practices, fraud-related holds, consumer dispute handling, and use of advanced analytics. Institutions operating nationally must reconcile these overlapping regimes while responding to fraud schemes that do not respect jurisdictional boundaries.

My testimony today reflects a legal practitioner's perspective across institutions of varying sizes and business models. Fraud has evolved rapidly in recent years. At the same time, many elements of the legal and supervisory framework were developed in an era when

fraud was slower, more siloed, and less technologically coordinated. The result is a growing tension between the speed and scale of emerging fraud trends and the structure of the regulatory architecture governing prevention efforts.

I appreciate the Committee's attention to these issues and look forward to discussing how policymakers can support effective fraud mitigation while preserving consumer protections, privacy, and fair access to financial services.

II. Emerging Fraud Trends Affecting Financial Institutions

Fraud is not a new phenomenon. Many of today's schemes are variations on themes that have existed for decades (*e.g.*, impersonation, forged instruments, confidence scams, and theft. What is new is how fraud is executed). Fraud is increasingly *industrialized, technology-enabled, cross-channel, and scalable*, with sophisticated coordination among actors and rapid adaptation to controls. In practice, that means financial institutions are confronting fraud that moves faster, spreads more quickly, and exploits seams between legal frameworks, payment rails, and institutional boundaries.

a. Check Fraud

Although checks are a longstanding payment instrument, check fraud has re-emerged as an "emerging trend" because the threat model has changed. Historically, check fraud often involved localized forgery or counterfeit checks presented in person. Today, the combination of organized theft, digital alteration tools, remote deposit channels, and predictable funds-availability timelines has created a materially different risk environment.

Key modern check-fraud typologies include:

1. **Mail Theft and Check Interception at Scale.**
   Organized criminal groups increasingly steal checks from mailboxes and postal facilities, exploiting the continued reliance of many consumers, small businesses, and government agencies on checks. Once obtained, checks can be altered, counterfeited, or used as templates to create additional fraudulent items.

2. **Check Washing and Alteration Using Modern Tools.**
   "Check washing" is not new, but it has become more scalable and precise. Fraudsters use readily available chemical and digital techniques to remove or modify payee names and amounts. In parallel, higher-quality imaging and printing technology makes counterfeit checks and altered items more convincing and more difficult to detect through traditional visual review.

3. **Remote Deposit Capture and Mobile Deposit Exploitation.**
   Remote deposit channels reduce friction for legitimate customers, but they also enable fraudsters to deposit altered or counterfeit items without the traditional

controls present in branch environments. A fraudulent item can be deposited quickly, sometimes across multiple institutions, before the receiving institution can validate authenticity.

4. **Funds Availability Timing and "Float" Exploitation.**
   Fraudsters are highly attuned to the gap between (i) when deposited funds become available and (ii) when final settlement and return processes confirm an item is fraudulent or uncollectible. That timing gap can be exploited to withdraw or transfer funds before the loss is identified. This dynamic is particularly challenging because institutions must balance the need to make funds available promptly for legitimate customers against the risk of subsidizing fraud.

5. **Account Opening and Mule Accounts Supporting Check Fraud.**
   Check fraud is often paired with "mule" accounts, which are accounts opened or controlled by fraud networks to receive proceeds and rapidly move funds. The growth of synthetic identity tools and compromised credentials has made mule-account creation easier, which in turn supports the scale of check fraud.

These modern conditions mean check fraud is not simply a "return to an old risk." It is an example of how longstanding schemes become "emerging" again when new channels, new tooling, and new operational constraints change the economics of fraud.

b. Social Engineering: Fraudulent Inducement at Scale

A defining feature of current fraud is the rise of scams in which consumers are manipulated into authorizing payments or disclosing credentials. This category of fraud is particularly difficult because the customer's action may appear "authorized" (and sometimes *are* "authorized") from a technical standpoint, even though it is the product of deception or coercion.

Common scam typologies include:

1. **Impersonation Scams.**
   Fraudsters impersonate banks, government agencies, law enforcement, employers, utilities, or well-known brands. They use phone spoofing, fake emails, cloned websites, and sometimes deepfake audio or video to appear credible. These scams often pressure consumers into urgently moving funds to "safe accounts" or providing one-time passcodes.

2. **Account Takeover Combined with Consumer Manipulation.**
   Fraudsters compromise credentials through phishing, malware, credential stuffing, SIM swaps, or social engineering. They then use the account access to initiate transfers, update contact information, or add payees. Sometimes they interact

directly with the consumer while simultaneously acting within the account, which can reduce the likelihood of timely intervention.

3. **Investment and Cryptocurrency Scams.**
   These scams leverage social media, messaging apps, and online advertising to lure consumers into fraudulent investment opportunities. The use of crypto exchanges and off-platform communications can complicate recovery and investigative pathways. Often, the initial "returns" shown to consumers are fabricated to induce larger transfers.

4. **Romance, Employment, and "Task" Scams.**
   Romance scams exploit personal trust. Employment and task scams offer "jobs" that require consumers to send funds, purchase gift cards, or move money through their accounts. These scams can generate multiple transfers over time, increasing total losses.

5. **Invoice and Business Email Compromise (BEC).**
   BEC schemes target businesses and individuals through spoofed or compromised email accounts, manipulating recipients into sending wires or ACH payments to fraudulent accounts. These schemes often rely on careful timing, knowledge of business relationships, and plausible documentation.

Modern scams are not isolated events. They are often multi-step playbooks. Fraudsters test a consumer's susceptibility, escalate pressure, and then route funds through mule networks. These scams create acute consumer harm, and they also impose operational and reputational costs on institutions even where the institution is not the ultimate bearer of the loss.

c. Fraud in Faster Payments and Cross-Rail Exploitation

As payment rails accelerate, fraud has adapted to exploit the reduced time available to detect and interrupt transactions. Faster payments improve efficiency and customer experience, but they also compress decision windows. In many cases, once funds are transmitted and received, recovery rates decline sharply. Even when a fraud scheme begins with a check deposit, card transaction, or account takeover, proceeds are often quickly transferred into faster rails (*e.g.*, ACH, real-time payments (RTP), wire transfers, or peer-to-peer platforms) and then dispersed across multiple accounts.

Key emerging typologies in faster-payment fraud include:

1. **Immediate Funds Availability and Settlement Compression.**
   Faster rails reduce float and settlement delays that historically provided time for review, verification, and potential intervention. Fraudsters exploit immediate funds availability by structuring transfers to minimize review triggers and rapidly

withdrawing or transferring funds once credited. Once funds are withdrawn in cash, converted to digital assets, or moved offshore, recovery rates decline significantly.

2. **Authorized Push Payment (APP) Fraud and Fraudulently Induced Transfers.**
In APP fraud patterns, a consumer initiates the payment, often in real time, after being deceived through impersonation, investment, emergency, or account-security scams. From a technical standpoint, authentication protocols may be satisfied. However, the authorization is obtained through manipulation or coercion. The speed of faster-payment rails means that funds may be credited and made available almost immediately, leaving only a narrow opportunity to detect anomalies or interrupt the transfer before onward movement.

3. **Rapid Cross-Rail Movement to Defeat Recovery Mechanisms.**
Fraud schemes frequently involve layering transactions across multiple rails. For example, proceeds from a compromised account may move from ACH to real-time payment, then to wire transfer, and ultimately to cash-out or conversion. Each rail has its own dispute, recall, and return processes, and rapid cross-rail movement is designed to outpace these mechanisms. This fragmentation complicates recovery and reduces the likelihood that any single institution can halt the full scheme. The result is a fragmentation of visibility, where no single institution sees the entire lifecycle of the fraud event.

4. **Multi-Institution Mule Networks and Asymmetric Information.**
Fraud actors leverage networks of mule accounts across multiple financial institutions. The sending institution may have limited visibility into whether the receiving account is newly opened, previously associated with fraud, or linked to suspicious device identifiers. Similarly, the receiving institution may lack context about the originating transaction. This asymmetric information combined with limited cross-institution sharing of device, network, or behavioral indicators creates exploitable gaps.

5. **Exploitation of Confirmation and Identity Gaps.**
Inconsistent implementation of payee verification, beneficiary confirmation, and account-validation tools can create confirmation gaps. Fraudsters direct victims to send funds to accounts that appear legitimate but are controlled by criminal networks. Where confirmation-of-payee mechanisms are not interoperable or universally deployed, consumers may receive limited warning before initiating irrevocable transfers.

6. **Compression of Detection and Escalation Windows.**
The operational reality of faster payments requires institutions to rely heavily on automated detection systems operating in real time. Manual review processes that were viable in slower settlement environments are increasingly impractical. Institutions must calibrate fraud controls to minimize false positives and consumer

friction while identifying high-risk transactions within seconds. This compressed timeline increases the importance of high-quality, timely risk signals and coordinated action across institutions.

The combination of speed, cross-rail layering, and multi-institution coordination makes faster-payment fraud particularly challenging. While faster rails are an important innovation, they alter the fraud calculus: prevention must occur earlier in the transaction lifecycle, and recovery options become more limited once funds are transmitted.

d. Identity-Centric Fraud: Synthetic Identity and Credential Abuse

Fraud increasingly hinges on weaknesses in identity proofing and authentication:

1. **Synthetic Identity Fraud.**
   Fraudsters combine real and fabricated identifiers to build "synthetic" personas that can pass certain checks. These identities may be aged over time, used to open accounts, obtain credit, and support mule networks.

2. **Credential Compromise and Account Takeover (ATO).**
   Credential theft is scaled through phishing kits, malware, and credential stuffing attacks using breached credentials. Account takeover is often paired with social engineering to defeat multi-factor authentication or to induce the consumer to disclose codes. Once access is obtained, funds are often moved quickly through multiple channels (*e.g.*, ACH, wire, instant payments, or card-based rails) frequently through networks of mule accounts.

3. **Document Fraud and Digital Identity Manipulation.**
   Fraudsters use manipulated IDs, synthetic documents, and increasingly sophisticated digital forgeries to pass onboarding checks and exploit remote channels.

III. The Challenges Financial Institutions are Facing with Emerging Fraud Trends

The fraud trends described above create operational, legal, supervisory, and economic challenges for financial institutions. These challenges are not limited to detecting individual fraudulent transactions; they implicate how institutions structure customer experience, deploy technology, allocate losses, coordinate across the financial system, and navigate overlapping regulatory regimes.

a. Balancing Fraud Prevention with Customer Experience and Access

Financial institutions must strike a difficult balance between preventing fraud and maintaining efficient, accessible services for legitimate customers. That balance is not

theoretical. It plays out in daily operational decisions across onboarding, funds availability, payment execution, and account servicing.

To combat emerging fraud trends, institutions are implementing increasingly sophisticated controls, including:

- Risk-based multi-factor authentication and step-up verification;
- Behavioral analytics evaluating device, geolocation, and transaction patterns;
- Real-time transaction monitoring systems designed to identify anomalies within seconds;
- Targeted transaction holds or outbound call-back verification for high-risk transfers;
- Enhanced identity verification and document authentication at onboarding;
- Participation in consortium-based fraud data or typology feeds where available.

At the same time, institutions are actively working to reduce unnecessary friction for legitimate customers. For example:

- Adaptive authentication limits additional verification steps to high-risk transactions rather than applying blanket requirements;
- Real-time customer alerts allow immediate confirmation or denial of suspicious activity;
- Streamlined digital onboarding processes rely on automated identity tools rather than manual documentation;
- Targeted holds are applied to specific transactions rather than entire accounts;
- Predictive analytics are continuously refined to reduce false positives.

These efforts reflect a fundamental economic reality: in a competitive marketplace, such as banking, customer experience is a key differentiator. Market economics strongly incentivize institutions to reduce fraud while minimizing friction. Consumers have choices, and institutions that impose excessive delays, unnecessary account restrictions, or repetitive authentication hurdles risk losing customers to competitors.

Fraud losses and fraud-prevention expenditures also carry broader economic consequences. Even when institutions absorb fraud losses directly, those losses affect capital allocation, operational costs, and investment decisions. Over time, fraud operates as a distributed cost across the customer base, impacting pricing, product availability, credit access, and innovation investment. Effective fraud prevention therefore serves not only institutional interests but systemic efficiency.

Accordingly, legal and regulatory frameworks should be structured to enable (rather than inhibit) good-faith fraud mitigation efforts. Institutions already possess strong commercial incentives to calibrate fraud controls responsibly. Policymaker and supervisory intent should focus on equipping institutions with the flexibility and clarity needed to deploy

proportionate, risk-based interventions without inadvertently creating new avenues for fraud or shielding fraudulent actors at the expense of legitimate customers.

b. Operating in Real Time with Compressed Decision Windows

Emerging fraud trends are unfolding in payment environments where the time available for intervention has materially compressed. Financial institutions increasingly must make high-stakes determinations about whether to allow, delay, flag, or block transactions.

This operational reality requires heavy reliance on automated systems, including machine learning models, behavioral analytics, and risk scoring. Traditional models that relied on extended manual review are often incompatible with real-time payment expectations.

The calibration challenge is significant. Systems that are overly sensitive can generate excessive false positives, increase customer friction, and elevate complaint volume. Systems that are overly permissive may allow rapid loss accumulation before controls adapt. Institutions must continuously refine detection models in response to evolving fraud typologies while documenting governance, validation, and performance.

The central dynamic confronting institutions is that fraud innovation is accelerating faster than the legal and supervisory structures designed to address it. Fraud actors increasingly leverage advanced technologies, including artificial intelligence and emerging AI agents capable of automating social engineering, credential harvesting, synthetic identity creation, and real-time transaction manipulation at scale. These tools significantly amplify the reach, speed, and sophistication of fraudulent activity. Fraud networks iterate rapidly, test vulnerabilities in real time, and operate without regulatory constraint. Financial institutions, by contrast, must respond within established statutory frameworks and supervisory expectations that were often developed for a slower and more contained threat environment. Bridging this speed and capability differential is one of the defining operational challenges in modern fraud prevention. Regulatory and oversight structures must therefore evolve in a manner that enables institutions to deploy comprehensive, technology-driven countermeasures commensurate with the commensurate technological capabilities necessary for modern fraud prevention.

c. Information Silos and Fragmented Visibility

Fraud is network-based and increasingly coordinated across institutions and platforms, yet detection often remains institution-specific.

No single institution typically sees:

- The full mule account network;
- The complete cross-rail movement of funds;
- Behavioral indicators flagged elsewhere;

- Parallel activity occurring across multiple institutions.

While limited information-sharing mechanisms exist, there is no comprehensive, real-time, legally streamlined framework for broad fraud-signal exchange across the ecosystem. As a result, institutions frequently operate with partial visibility, while fraud networks operate with coordinated intelligence.

Modern fraud networks are multi-actor, cross-institutional, and often cross-border. Tactics and scripts are shared rapidly across digital channels. Attack methods are tested, refined, and redeployed. What appears to be an isolated anomaly at one institution may be part of a broader coordinated scheme visible only when activity is viewed across the system. This asymmetry, coordinated fraud networks versus fragmented institutional visibility, remains a core structural challenge.

d. Legal and Supervisory Uncertainty

Institutions must deploy fraud controls within a layered legal and supervisory environment that was not constructed for today's real-time, cross-channel fraud ecosystem.

They must evaluate, often simultaneously:

- When fraud-related transaction holds are permissible and for how long;
- Whether funds must be made available under Regulation CC notwithstanding emerging fraud indicators, and when exception holds are appropriately invoked in light of modern check fraud dynamics;
- How Regulation E applies to fraudulent transfers;
- Whether certain fraud-signal sharing practices implicate FCRA obligations;
- How fraud detection models intersect with notice requirements and fair lending standards;
- Whether transaction denials or delays create UDAAP exposure.

Supervisory expectations introduce additional cross-pressures. Institutions may be criticized for elevated fraud losses, yet may also face scrutiny when aggressive controls increase friction or delay funds. In the context of check fraud, for example, institutions must reconcile prompt funds-availability requirements with the operational reality that altered or counterfeit items may not be identified until after provisional availability has been provided.

Navigating these competing expectations requires substantial legal analysis, documentation, governance, and resource allocation.

Even where statutory authority exists, uncertainty about supervisory interpretation can create hesitation in deploying more assertive fraud interventions. The result can be predictability that sophisticated fraud actors exploit.

e. Technology Deployment and Governance Complexity

The sophistication of modern fraud requires equally sophisticated detection tools. Artificial intelligence, behavioral biometrics, predictive analytics, and cross-channel risk scoring are increasingly essential components of effective fraud programs.

However, deploying these tools entails significant governance obligations. Institutions must address:

- Model validation and ongoing performance monitoring;
- Explainability and documentation standards;
- Vendor oversight and third-party risk management;
- Cybersecurity protections;
- Ongoing monitoring for perceived disparate impact.

Governance is critical to responsible innovation. However, legal standards should be structured to enable responsible deployment of fraud controls. They should not impose incremental costs, delays, or procedural burdens that fail to enhance consumer protection and, in practice, advantage fraud actors over legitimate financial institutions and their customers.

f. Resource Constraints for Community Institutions

Community banks and credit unions play an essential role in financial inclusion, small-business lending, and local economic stability. However, they often operate with smaller fraud teams, more limited in-house analytics capabilities, and less access to real-time typology intelligence than larger institutions. Many rely heavily on third-party vendors for fraud detection and monitoring.

Fraud actors routinely probe for the weakest point in the financial ecosystem. When smaller institutions lack access to robust information-sharing networks, cross-institution fraud signals, and scalable detection tools, they can become disproportionate targets for mule accounts, check fraud, and scam-driven payment flows.

Strengthening information-sharing frameworks and providing clear statutory safe harbors would benefit the entire financial system, but the impact would be particularly meaningful for community banks and credit unions. Broader access to shared fraud intelligence, standardized risk indicators, and legally certain collaboration mechanisms would allow smaller institutions to participate more effectively in coordinated defense efforts without bearing unsustainable compliance costs.

System-wide resilience depends on ensuring that fraud prevention capabilities are not concentrated solely in the largest institutions. When fraud losses concentrate in under-

resourced segments of the market, the consequences extend beyond individual institutions. Losses and remediation costs reverberate across the broader financial system, affecting pricing, access, and consumer trust. A framework that enables scalable collaboration and technological adoption across institutions of all sizes strengthens financial stability as a whole.

IV. Legal and Regulatory Framework Governing Fraud Prevention

a. Statutes

Several federal statutes directly or indirectly govern fraud prevention and loss allocation.

Expedited Funds Availability Act (EFAA) and Regulation CC.
Regulation CC governs funds availability schedules and check return processes. While designed to ensure timely access to funds, funds-availability requirements interact directly with modern check fraud dynamics, particularly in environments involving remote deposit capture and organized mail theft.

Fair Credit Reporting Act (FCRA).
FCRA governs the furnishing, use, and sharing of consumer report information. Fraud detection tools that rely on consortium data, negative file information, device identifiers, or certain identity-verification processes may implicate FCRA definitions of "consumer report," "furnisher," or "consumer reporting agency." Institutions must evaluate whether particular data-sharing arrangements fall within FCRA's scope and whether fraud-related decisions (*e.g.*, account closures, onboarding denials, or transaction restrictions) trigger adverse action notice requirements.

As a result of FCRA's definitions are broad and fact-specific, institutions must carefully structure fraud-information sharing and consortium participation to ensure compliance with permissible purpose, accuracy, and dispute-resolution obligations.

Equal Credit Opportunity Act (ECOA).
ECOA prohibits discrimination in credit transactions and requires creditors to provide adverse action notices when credit is denied or other adverse credit decisions are made. When fraud detection tools influence onboarding decisions, credit approvals, account access, or transaction authorizations tied to credit products, institutions must evaluate whether those decisions constitute adverse action under ECOA and its implementing Regulation B.

If an adverse action occurs, institutions are generally required to provide a statement of reasons that is specific and accurate. In fraud-related contexts, this can present operational complexity. Fraud detection models often rely on dynamic, multi-factor risk scoring, behavioral indicators, device analytics, or cross-channel typology signals.

Translating these risk determinations into clear, legally sufficient reasons for decline requires careful documentation and model governance.

Institutions must also evaluate potential fair lending implications, including whether fraud detection models could produce perceived disparate impact across protected classes. Even when a model is designed solely for fraud prevention and not credit risk assessment, its outputs may affect access to credit or account functionality, thereby implicating ECOA compliance considerations.

Gramm-Leach-Bliley Act (GLBA).
GLBA imposes privacy and safeguarding obligations, shaping how institutions collect, use, and share consumer financial information. Fraud prevention often depends on data sharing across entities and platforms, which must be evaluated against GLBA's privacy restrictions and exceptions.

Bank Secrecy Act (BSA), Anti-Money Laundering (AML), and Section 314(b).
Under the BSA, financial institutions are required to maintain anti-money laundering programs, monitor for suspicious activity, and file Suspicious Activity Reports (SARs) where appropriate. These obligations often capture fraud-related conduct, particularly when fraud proceeds are moved through networks designed to obscure origin and ownership.

Section 314(b) of the USA PATRIOT Act permits financial institutions to share information with one another, under specified conditions, for purposes of identifying and reporting activities that may involve money laundering or terrorist financing. In practice, some institutions utilize Section 314(b) frameworks to facilitate limited information sharing related to fraud schemes that may also implicate financial crime concerns.

However, Section 314(b) is structured around AML objectives and includes procedural and definitional limitations. As fraud schemes increasingly overlap with money movement typologies traditionally associated with AML risk, institutions must evaluate carefully how and when fraud-related information sharing fits within the 314(b) safe harbor framework.

Electronic Fund Transfer Act (EFTA) and Regulation E.
EFTA establishes consumer protections for electronic fund transfers, including error resolution procedures and liability limitations for unauthorized transactions. In practice, Regulation E plays a central role in how institutions allocate losses arising from account takeover and certain types of fraudulently induced transfers. Institutions must evaluate whether a transaction qualifies as "unauthorized," the timeliness of consumer notice, and the scope of required investigation and credit.

Truth in Lending Act (TILA) and Regulation Z.
For credit card transactions, TILA provides liability limitations for unauthorized use and establishes billing error procedures. As fraud increasingly spans debit, credit, and hybrid

products, institutions must apply different statutory frameworks depending on product structure (even when fraud typologies are operationally similar leading to differing outcomes depending on the product involved in the fraud).

b. Regulatory Guidance

Beyond statutory text, regulators have issued guidance addressing fraud risk management, cybersecurity, third-party oversight, and model governance.

Federal banking agencies have articulated expectations regarding:

- Risk-based authentication and layered security programs;
- Information security standards and safeguarding obligations;
- Third-party vendor management and oversight;
- Model risk management frameworks for advanced analytics;
- Consumer compliance management systems.

Agencies have also issued statements, interpretive guidance, and frequently asked questions addressing payments fraud, faster-payment systems, scam typologies, and consumer dispute obligations. While these materials provide important supervisory context, they are often issued outside of formal notice-and-comment rulemaking processes.

In some instances during the prior administration, interpretive guidance and FAQs were viewed by institutions as expanding statutory frameworks beyond their original scope. For example, FAQs interpreting EFTA and Regulation E addressed fraudulently induced transfers in ways that some institutions believed extended liability expectations beyond the statutory text, without formal rulemaking. Similarly, interpretive positions under Regulation Z were perceived as potentially extending coverage to products or operational practices not clearly contemplated by the statute or implementing regulation.

These developments contribute to interpretive uncertainty. Institutions must navigate evolving guidance while ensuring compliance with statutory text, and must assess whether informal supervisory materials effectively alter operational expectations without the clarity and procedural safeguards associated with rulemaking. That uncertainty is particularly consequential in fraud contexts, where decisions must often be made in real time and under compressed timelines.

c. Supervisory Expectations

In practice, supervisory expectations play a central role in shaping fraud-prevention programs. While statutes and regulations should set legal requirements, standards are often defined through examination processes, supervisory communications, and enforcement posture.

Institutions are examined not only for technical compliance with statutory requirements, but also for the effectiveness of their risk management, governance, and control environments. Examiners may evaluate:

- Fraud loss metrics and trend data;
- Customer complaint volumes and narratives;
- Model performance, validation, and documentation;
- Fair lending implications of fraud detection models;
- UDAAP risk associated with transaction denials, account restrictions, or delays;
- Vendor oversight and third-party fraud detection arrangements;
- Error resolution determinations under EFTA and Regulation E;
- Adverse action notices and stated reasons under ECOA and Regulation B.

Supervisory scrutiny can arise both when fraud losses increase and when institutions implement assertive fraud controls that create customer friction. Institutions may be required to explain why particular fraud events were not prevented, while simultaneously being asked to justify transaction holds, onboarding denials, or account closures implemented to mitigate risk. In some instances, institutions face pressure to provide highly specific reasons for fraud-related decisions, which raises concerns that detailed disclosures could inadvertently reveal sensitive fraud-detection methodologies or provide information that sophisticated actors could exploit.

Examination findings can carry significant operational and reputational consequences, which leads institutions to calibrate fraud programs not only to statutory requirements but also to perceived supervisory posture.

d. State Laws

Institutions operating nationally must implement fraud controls in a manner that fully complies with federal statutes, regulatory guidance, supervisory expectations, and state consumer protection and privacy regimes. These frameworks serve important and legitimate purposes, including safeguarding consumer rights and protecting sensitive financial information. At the same time, differences in scope, interpretation, and enforcement priorities across jurisdictions can create operational complexity for institutions attempting to deploy consistent, real-time fraud prevention programs.

This complexity affects:

- Information sharing practices;
- Fraud-related account restrictions;
- Data retention policies;
- Consumer notification requirements;
- Use of analytics and risk modeling.

Fraud schemes operate without regard to jurisdictional boundaries. Financial institutions, by contrast, must ensure that controls comply with overlapping federal and state requirements. This legal fragmentation can introduce delay or hesitation in implementing collaborative fraud solutions.

V. Areas Where Current Law Constrains Fraud Prevention Efforts

The legal framework governing fraud prevention reflects important consumer protection, privacy, and fairness objectives. However, as fraud has become faster, more coordinated, and more technology-enabled, certain features of current law (and, in some instances, its interpretation and supervisory application) can constrain timely fraud intervention. These constraints arise most acutely in (1) information sharing, (2) liability and dispute frameworks, (3) funds availability rules, (4) supervisory and UDAAP risk, and (5) the ability to deploy technology consistently across jurisdictions.

a. Constraints on Information Sharing and Collaborative Fraud Mitigation

Modern fraud is network-based, and effective prevention increasingly depends on the ability to identify mule accounts, device patterns, typologies, and risk signals across institutions. Current law provides pathways for sharing in limited circumstances, but those pathways are often fragmented, uncertain, or not designed for real-time fraud mitigation.

FCRA definitional and recharacterization risk.
Institutions may hesitate to share certain fraud indicators such as signals tied to identity attributes, device identifiers, or behavior patterns due to concern that sharing could be characterized as furnishing a "consumer report" or creating consumer reporting obligations. This uncertainty can discourage the very kind of consortium-based sharing that is most effective against coordinated fraud networks.

Section 314(b) Limitations in Modern Fraud Contexts.
Section 314(b) of the USA PATRIOT Act permits voluntary institution-to-institution information sharing under specified conditions for purposes related to identifying and reporting money laundering or terrorist financing. While this framework can support certain fraud-related coordination, it was designed primarily around AML objectives and contains definitional and procedural requirements that do not always align with modern, high-velocity fraud typologies, particularly scam-driven authorized payments and other non-AML fraud patterns.

As fraud schemes increasingly overlap with AML-related behaviors such as mule accounts and layered transactions, institutions must carefully evaluate whether fraud-related information sharing falls within the scope of Section 314(b). In time-sensitive scenarios, institutions may also assess whether the framework is operationally suited for real-time fraud mitigation. This can result in uncertainty

about the extent to which 314(b) provides a comprehensive solution for coordinated fraud defense.

GLBA privacy and safeguarding considerations.
Institutions must evaluate whether and how nonpublic personal information can be shared for fraud prevention purposes, including whether the sharing fits within available exceptions and how notice and opt-out requirements may apply in particular contexts. These requirements can slow or narrow the sharing of fraud signals that are most useful when transmitted quickly and at scale.

The practical result is that fraud networks operate across institutions with high coordination, while institutions often face legal uncertainty about whether they can share the risk signals needed to identify those networks quickly.

b. Funds Availability and the Operational Reality of Modern Check Fraud

Check fraud illustrates a core friction point: fraud prevention often requires time, while funds availability rules and customer expectations demand speed.

Institutions must balance prompt funds availability with the reality that counterfeit, altered, or otherwise uncollectible items may not be identified until return and adjustment processes occur. In a world of remote deposit capture, mail theft, and sophisticated alteration, the time gap between deposit and final collectability is frequently the window fraudsters exploit.

Even where Regulation CC provides exceptions and hold authorities, operational and supervisory uncertainty about when those exceptions are appropriate, and how they will be evaluated after the fact, can make institutions reluctant to apply holds as aggressively as fraud trends might otherwise warrant.

c. Supervisory and UDAAP Risk That Can Discourage Proactive Intervention

Institutions seeking to implement robust fraud controls must simultaneously manage UDAAP, and complaint-related risk. Managing these risks can create a challenging dynamic in which institutions face scrutiny both when fraud losses occur and when preventive controls result in customer friction, transaction delays, or account restrictions affecting users.

UDAAP risk in fraud controls. Fraud controls can trigger allegations of unfairness when they delay funds, restrict account access, or create inconveniences for consumers. Institutions must therefore design controls that are risk-based, targeted, and well-governed. At the same time, fraud prevention requires fast action and relies on imperfect information.

Inconsistent Supervisory Interpretation. In practice, the application of statutory and regulatory text can be influenced by supervisory posture. At times, institutions report that supervisory staff apply interpretations that extend beyond the requirements of the governing statute or implementing regulation. When expectations are perceived as broader than the underlying legal framework, institutions may experience uncertainty in determining the appropriate scope of fraud controls. This can create hesitation around reasonable, good-faith intervention measures, particularly where institutions are concerned that a risk-based hold, transaction denial, or account restriction may later be second-guessed despite being supported by documented fraud indicators.

This is not an argument for weakening consumer protection. It is an argument for ensuring that supervision and interpretive approaches align with statutory text and with the legitimate interests of preventing fraud so that the law does not inadvertently become a tool that fraud actors can exploit.

d. Liability Allocation Challenges in Multi-Platform Fraud Environments

Fraud today frequently involves fraudulently induced payments, credential compromise, and multi-platform transaction flows that do not fit neatly within older authorized versus unauthorized liability categories.

Modern fraud schemes frequently span multiple institutions, non-bank payment providers, digital wallets, fintech platforms, and intermediaries. A single scam event may involve credential compromise at one institution, initiation through a peer-to-peer platform, rapid movement across payment rails, and ultimate withdrawal at a separate institution. In these multi-party scenarios, determining which entity bears which investigative, reimbursement, or notice obligations can be legally and operationally complex.

Institutions must assess at what point an "error" arises under applicable statutes, which entity is responsible for conducting the investigation, and how liability should be allocated when funds move quickly across platforms. In practice, institutions often have limited visibility into the full lifecycle of the transaction, particularly where non-bank providers or intermediaries control portions of the customer interface or transaction flow.

CFPB guidance has emphasized that consumer protections may apply even when a non-bank peer-to-peer provider or wallet is involved. While protecting consumers in multi-party environments is important, this interpretive approach can place primary investigative and reimbursement pressure on depository institutions that may not control the originating interface, authentication environment, or transaction design. Banks and credit unions are therefore required to resolve disputes and make liability determinations based on incomplete information while coordinating across entities with differing legal obligations and operational timelines.

The constraint is not the existence of consumer protections, which are fundamental. Rather, the challenge is that statutory frameworks built around bilateral transactions are increasingly applied to multi-platform ecosystems. When liability expectations are expanded without corresponding clarity regarding inter-institution responsibility and information sharing, institutions' ability to interrupt suspicious transactions promptly can be diminished by heightened and asymmetric liability risk.

e. State Privacy and Emerging State AI Laws Create Additional Friction for Modern Fraud Technology

As institutions increasingly rely on advanced analytics, behavioral biometrics, and machine learning to detect fraud in real time, state-level legal fragmentation creates practical obstacles.

State data-use constraints. State data laws may limit collection, processing, and sharing of data elements that are important for fraud prevention, including, consumer specific information, behavioral signals, and cross-platform typology analytics. Institutions must navigate varying definitions, exemptions, and consumer rights requirements across jurisdictions.

Emerging state AI laws and algorithmic governance mandates. State AI laws and proposals increasingly impose requirements relating to automated decision systems (which are sometimes defined extremely broadly). Fraud prevention tools frequently depend on rapid iteration and continuous tuning in response to new typologies. Divergent state-level AI requirements can frustrate the ability of institutions to deploy and update fraud models quickly and consistently.

Recent federal policy developments also reflect a recognition of this tension. For example, President Trump's executive actions regarding AI policy emphasize a national approach designed to reduce barriers to AI adoption and address state-level regulatory obstruction, reflecting an effort to promote innovation and deployment across sectors. The executive order underscores a policy direction that lawmakers should further advance through durable statutory clarity.

The practical risk is that fraud evolves in days or weeks, while institutions face a patchwork of governance and compliance obligations that may slow adoption of new tools, deter experimentation, or force one-size-fits-none model constraints that ultimately favor fraudulent actors rather than legitimate customers. This dynamic is particularly acute for community banks and credit unions, which often lack the resources to engage in prolonged supervisory disputes or to challenge expansive interpretations that exceed statutory text. In practice, smaller institutions may feel compelled to acquiesce to aggressive (many times incorrect) supervisory positions because the cost of resistance can exceed their available compliance capacity. The result is not only regulatory

uncertainty, but a disproportionate burden on community institutions that are critical to local economies and financial inclusion.

VI. Opportunities for Policymakers to Support Fraud Prevention

The fraud environment described above requires more than incremental guidance. It requires targeted statutory clarity, carefully structured safe harbors, and explicit direction to regulators to align supervisory posture with technological reality.

Congress has the opportunity to modernize existing frameworks in ways that preserve core consumer protections while enabling institutions to prevent fraud effectively and in real time. The following measures provide a legislative roadmap.

a. Establish a Fraud-Prevention Safe Harbor Under the FCRA

Congress should provide an explicit safe harbor allowing financial institutions and regulated entities to share fraud-risk indicators for prevention purposes.

Such a provision could:

- Clarify that sharing limited fraud signals (*e.g.*, mule account identifiers, device fingerprints, behavioral risk scores, or typology flags) solely for fraud prevention does not constitute furnishing a consumer report;
- Provide immunity from civil liability for good-faith fraud-signal sharing within defined parameters;
- Authorize standardized fraud consortium frameworks;
- Encourage development of interoperable fraud signal exchange systems.

This clarification would directly address fragmented visibility challenges and would complement, but not replace, AML-focused mechanisms under Section 314(b).

b. Clarify and Expand Section 314(b) for Fraud Coordination

Congress should modernize Section 314(b) to explicitly encompass coordinated fraud prevention, including scam networks and mule-account activity.

Legislative improvements could:

- Clarify that sharing information related to organized fraud schemes qualifies as permissible activity;
- Streamline registration and certification procedures to facilitate real-time sharing;
- Provide liability protection for good-faith sharing related to fraud detection and mitigation;

- Encourage cross-rail fraud coordination between banks, credit unions, and regulated payment providers.

Modern fraud networks use layered transactions and mule accounts that overlap with AML typologies. Clarifying 314(b) would reflect that operational reality.

c. Provide Safe Harbors for Risk-Based Fraud Controls Under ECOA and TILA

Fraud detection programs increasingly intersect with account access, onboarding, and transaction approvals involving credit products. While ECOA and TILA provide critical consumer protections, modern fraud typologies create ambiguity about how those frameworks apply to risk-based fraud interventions.

Congress could consider the following clarifications:

1. **Clarify that fraud-based interventions are distinct from creditworthiness determinations.**
   Statutory language could confirm that actions taken based on documented fraud-risk indicators do not constitute adverse action under ECOA where the decision is not based on creditworthiness.

2. **Protect sensitive fraud detection methodologies.**
   Congress could provide that where an adverse action notice is required, institutions are not obligated to disclose specific fraud-detection algorithms, typologies, or security controls in a manner that would compromise system integrity or facilitate evasion.

3. **Provide a safe harbor for commercially reasonable fraud controls.**
   A statutory safe harbor could protect institutions that deploy validated, risk-based fraud detection models designed to prevent identity theft, account takeover, or scam-related losses, provided such models are implemented in a manner consistent with fair lending laws.

4. **Reinforce statutory scope boundaries under TILA and Regulation Z.**
   Congress could clarify, through express statutory language where necessary, the categories of products that fall within or outside TILA's scope. For example, providing explicit statutory confirmation regarding products such as certain earned wage access arrangements or defined pay-in-four structures would reduce uncertainty and avoid expansion through informal interpretation rather than rulemaking.

These measures would preserve core fair lending and disclosure protections while reducing ambiguity around fraud-prevention tools and product scope. Clarifying the

distinction between fraud mitigation and credit underwriting would enhance regulatory certainty and allow institutions to act decisively against fraudulent activity without undermining consumer rights.

d. Establish a Dynamic Commercially Reasonable Security Safe Harbor

Many existing statutes rely, either explicitly or implicitly, on concepts such as "reasonable" or "commercially reasonable" security. However, what constitutes commercially reasonable fraud prevention evolves rapidly as technology, threat vectors, and detection capabilities advance.

Congress could direct the relevant federal regulators to conduct periodic, technology-focused studies examining current fraud typologies, authentication methods, behavioral analytics, artificial intelligence applications, and inter-institution information-sharing tools. Based on those studies, regulators could be required to articulate and regularly update a commercially reasonable security standard for fraud prevention.

Congress could further codify a cross-statute safe harbor providing that:
An institution that implements and maintains a documented, risk-based fraud prevention program consistent with regulator-defined commercially reasonable security standards shall not be subject to liability *solely* because a fraud event occurred, provided the institution acts in good faith and in accordance with those standards.

Such a framework could incorporate:

- Adoption of industry-standard authentication and identity verification protocols;
- Use of adaptive and AI-driven fraud detection systems;
- Participation in authorized information-sharing frameworks;
- Periodic independent validation and performance testing of fraud controls;
- Ongoing model governance and bias monitoring consistent with fair lending principles.

Requiring regulators to study and understand emerging technological capabilities before criticizing institutional practices would promote informed regulation and supervision. A regularly updated safe harbor would reduce hindsight-based litigation and supervisory second-guessing, while encouraging continued investment in advanced fraud prevention tools.

This approach would not weaken consumer protections. Rather, it would align liability expectations with evolving security standards and create regulatory certainty for institutions acting in good faith to protect consumers and the financial system.

e. Direction to Regulators

Legislative modernization alone will not resolve the structural challenges described above. Effective fraud prevention also depends on regulatory alignment, procedural discipline, and informed supervision. Congress can provide clear direction to ensure that regulatory implementation supports, rather than constrains, good-faith fraud mitigation.

1. **Reinforce Statutory Boundaries and Procedural Discipline.**
   Congress should reaffirm that material expansions of statutory liability or coverage must occur through legislation or formal notice-and-comment rulemaking.

   In recent years, institutions have experienced significant operational shifts through FAQs, supervisory statements, and interpretive materials (particularly in the context of Regulation E and fraudulent transfers). While agencies appropriately issue interpretive guidance, substantive changes to statutory liability standards should not occur through informal mechanisms that lack procedural safeguards, economic analysis, and public input.

   Congress could:

   - Require that significant changes to liability allocation or product coverage under EFTA, TILA, and other statutes proceed through formal rulemaking;
   - Clarify that FAQs and supervisory guidance do not independently alter statutory scope;
   - Direct agencies to review prior informal interpretations that materially expand statutory obligations absent rulemaking.

   This would restore transparency, ensure accountability, and provide institutions with predictable legal standards in fast-moving fraud environments.

2. **Provide Guardrails for Supervisory Use of UDAAP and ECOA**

   Congress should clarify that core consumer protection authorities are not intended to deter documented, risk-based fraud controls.

   Statutory direction could provide that:

   - Temporary holds, transaction delays, enhanced authentication, or account restrictions implemented pursuant to commercially reasonable fraud prevention programs do not constitute unfair or abusive practices absent bad faith, discriminatory intent, or systemic misconduct;
   - Adverse action requirements under ECOA apply to creditworthiness determinations and should not be interpreted to require disclosure of sensitive fraud-detection methodologies;

- Institutions shall not be deemed to engage in unfair practices solely because fraud controls introduce incidental friction when implemented in good faith.

Such clarification would preserve robust consumer protections while reducing hesitation around reasonable intervention measures. UDAAP should remain a tool to prevent genuine consumer harm, not a source of uncertainty that discourages proactive fraud mitigation.

3. **Require Technology-Informed Supervision and Establish a Dynamic Commercially Reasonable Safe Harbor**

Fraud prevention is increasingly dependent on advanced authentication, behavioral analytics, artificial intelligence, and cross-institution coordination. Regulatory expectations must evolve in parallel with technological capabilities.

Congress should require federal regulators to conduct periodic, technology-focused studies addressing:

- Emerging fraud typologies and scam evolution;
- The effectiveness and limitations of AI-driven fraud detection systems;
- Cross-rail and multi-platform coordination challenges;
- The interaction between fraud prevention tools and statutory liability frameworks.

Based on these studies, regulators should be directed to articulate and regularly update a commercially reasonable security standard for fraud prevention. Congress could further provide that institutions implementing documented, risk-based fraud programs consistent with regulator-defined commercially reasonable standards receive a liability safe harbor against claims based solely on the occurrence of fraud.

Regulatory expectations should be grounded in an informed understanding of technological tools, operational constraints, and evolving threat environments. A dynamic safe harbor framework would reduce hindsight-based enforcement and litigation while encouraging continued investment in advanced fraud mitigation systems.

4. **Promote National Consistency in AI Governance for Fraud Detection**

Fraud detection increasingly relies on artificial intelligence, adaptive modeling, and real-time analytics. Emerging state-level AI regulatory regimes risk creating fragmentation that slows deployment, increases compliance cost, and complicates model iteration across jurisdictions.

Recent executive action has emphasized the importance of coordinated national AI policy. Congress has an opportunity to build on that direction by:

- Establishing harmonized federal governance standards for AI systems used in fraud detection;
- Providing preemption or safe harbor protections where institutions comply with federal AI oversight requirements;
- Requiring transparency, documentation, and bias mitigation safeguards that preserve fair lending protections without imposing conflicting state mandates.

A coherent national framework would allow institutions of all sizes to deploy rapidly improving fraud technologies responsibly, while maintaining appropriate oversight and consumer safeguards.

Regulators play an essential role in protecting consumers and maintaining financial stability. Clear congressional direction that reinforces statutory boundaries, encourages procedural discipline, and aligns supervision with technological reality would strengthen that role. A regulatory environment grounded in clarity and informed oversight will better equip financial institutions to combat increasingly sophisticated fraud without undermining core consumer protections.

Taken together, these reforms would:

- Clarify fraud-signal sharing under FCRA and 314(b);
- Protect risk-based fraud controls under ECOA, TILA, and UDAAP;
- Codify commercially reasonable fraud-prevention safe harbors;
- Align regulatory guidance and supervision with statutory text;
- Promote nationally consistent AI governance.

The objective is not deregulation. The objective is to ensure that the law does not inadvertently create new avenues for fraud or favor fraudulent actors over legitimate consumers and financial institutions.

Fraud prevention requires speed, coordination, and technological adaptation. The legal framework should enable those attributes while preserving the core consumer protections that Congress has rightly established.

VII. Conclusion

Fraud today is not episodic, localized, or unsophisticated. It is coordinated, technology-enabled, cross-channel, and adaptive. Fraud networks iterate rapidly, share tactics in real time, and exploit structural seams between institutions, payment rails, and regulatory frameworks. They operate without regard to jurisdictional boundaries or statutory silos.

Financial institutions, by contrast, must operate within layered federal and state statutes, regulatory guidance, supervisory expectations, privacy constraints, and evolving governance standards. They must navigate FCRA data-sharing constraints, Regulation CC funds-availability requirements, Section 314(b) information-sharing parameters, TILA and Regulation Z obligations, EFTA and Regulation E liability frameworks, and UDAAP standards simultaneously and under compressed decision timelines. They are expected to reduce fraud losses, protect consumers, deploy advanced technology responsibly, avoid disparate impact, maintain seamless customer experiences, and absorb losses when fraud succeeds while operating within statutory frameworks developed in a different fraud era.

Despite these constraints, institutions have strong independent incentives to prevent fraud. Customer trust is foundational. In a competitive marketplace, customer experience is a key differentiator. Institutions that fail to prevent fraud or that impose excessive friction lose customers. Fraud losses, investigation costs, and compliance expenditures do not disappear; they ultimately influence pricing, access, and innovation across the financial system. Fraud functions as a systemic cost that affects every legitimate participant in the financial ecosystem.

The question before policymakers is not whether to protect consumers. It is how to ensure that the legal and supervisory framework enables institutions to protect consumers effectively in a modern threat environment.

The recommendations outlined in this testimony reflect several core principles:

1. **Safe harbors for good-faith fraud prevention.**
   Institutions that implement commercially reasonable, risk-based fraud controls should have legal certainty that those efforts will not be second-guessed solely because fraud occurred or because customer friction was unavoidable.

2. **Modernized information sharing.**
   Coordinated fraud requires coordinated defense. Clarifying and strengthening Section 314(b) to explicitly encompass organized fraud activity and providing explicit safe harbors for fraud-signal sharing, would materially improve system-wide resilience.

3. **Alignment of funds-availability rules with modern fraud dynamics.**
   Regulation CC was designed to promote timely access to funds, but modern check fraud exploits predictable timing gaps. Policymakers should ensure that institutions retain appropriate authority to apply risk-based holds when warranted by evolving fraud typologies.

4. **Clarity over ambiguity.**
   Statutory standards—particularly under EFTA, Regulation CC, FCRA, ECOA, and TILA—should be applied consistent with their text and expanded only through transparent legislative or rulemaking processes.

5. **Supervisory alignment with technological reality.**
   Regulators should evaluate fraud prevention efforts based on informed understanding of evolving technology and the operational constraints of real-time payment systems. Criticism untethered from technological context discourages innovation rather than promoting consumer protection.

6. **National coherence in AI governance.**
   Fraud detection increasingly depends on advanced analytics and machine learning. A fragmented regulatory environment that slows adoption or imposes inconsistent mandates across jurisdictions will disadvantage legitimate institutions while fraud networks continue to evolve.

Effective fraud prevention and strong consumer protection are complementary objectives. A legal framework that enables timely, collaborative, technology-driven intervention will reduce losses, improve trust, and strengthen financial system integrity.

Fraud will continue to evolve. The legal framework must evolve with it.

Chairman BARR. Thank you. The gentleman yields back.

Last but not least, Mr. Rust, you are now recognized for 5 minutes.

STATEMENT OF ADAM RUST, DIRECTOR OF FINANCIAL SERVICES, CONSUMER FEDERATION OF AMERICA

Mr. RUST. Chairman Barr, Ranking Member Foster, and members of the committee, thank you for the opportunity to testify today.

My name is Adam Rust. I am director of financial services for the Consumer Federation of America.

CFA is a nonprofit organization dedicated to serving the consumer interests, with 215 nonprofit coalition members across the country, and we house Veteran Saves and Military Saves to help approximately 240,000 individuals build wealth.

Today, I want to talk about scams which are among the most serious threats facing consumers today. You have heard about the large numbers of losses. The numbers are truly much larger because so many scams are never reported.

Scams affect people in every congressional district, of every age, young, old, urban, rural, civilian and servicemember.

I want to focus my testimony on five things Congress can do.

First, attacks on the CFPB must end. The CFPB is the primary Federal agency with the mandate and expertise for consumer financial protection and authority for Electronic Fund Transfer Act (EFTA) and Unfair, Deceptive, or Abusive Acts or Practices (UDAAP). Its Complaint Data base receives complaints from harmed consumers. This information can be shared with law enforcement and other concerned parties.

When consumers are harmed, the CFPB has sent a clear signal: When companies offer unsafe products, there will be consequences, but that signal has been silenced by dropping enforcement, gutting supervision, and firing staff. The consumers' champion has been taken off the beat and Congress overturned the rule requiring supervision of payment apps and digital wallets.

Consumer relief rates have dropped precipitously, from approximately 50 percent 2 years ago to now less than 1 percent.

Second, EFTA is broken for scam victims. EFTA was written in 1978 when electronic theft meant a stolen ATM card. Today's criminals coerce victims into authorizing transfers where there is little recourse under the law.

CFA supports the Protecting Consumers from Payment Scams Act, which would expand coverage to wires, call for shared liability, and create protections against induced transfers. The bill will modernize EFTA to actually address how scams work now.

Third, every company across the payment journey should be accountable and a part of the solution. For every scam, there is a destination: a bank or a payment app of the criminal. Criminals deliberately target FIs with weak fraud detection to help them find ways to open accounts and receive funds and then later move it on for funnel accounts.

Suspicious Activity Report (SAR) filings on funnel accounts have increased fourfold since 2020, and bank fintech partnerships, such

as the example of the Synapse case, are a critical point of vulnerability.

True, send-side FIs do not have the full picture. Receive-side FIs and payment networks have a unique line of sight with directory information as well. Let us connect those sight lines.

More use of real-time AI, better information sharing, and possibly the expulsion of stubbornly risk-leaning FIs would improve the ecosystem's safety for everyone. The U.K. has shown that shared liability works.

The problem has many surfaces, and every actor—banks, nonbank apps, networks, platforms, telcos—all must have skin in the game.

Fourth, we must bridge the gap between illicit finance enforcement and consumer protection. The types of criminal organizations that have historically been the subject of Bank Secrecy Act (BSA) and anti-money laundering (AML) violations are now open for a new line of business: scamming Americans.

Yet, BSA enforcement actions and consumer protection work have been in silos. That should change. The CFPB should be in the room, and penalties resulting from violations should include remedies for scam victims.

Fifth, we should make efficient use of SARs. Much of the most useful information in a SAR is buried in narrative fields, where law enforcement has difficult times to access it at scale.

To help law enforcement, FinCEN should migrate more data to structured formats and add a scam check box with device and account identifiers to permit appending and tracking across financial institutions.

The dark web is not calling for higher reporting thresholds. Neither should we. It would be blind for law enforcement to many transactions, including some that affect lower-dollar transactions such as teen sextortion.

The tools to fix this problem exist. Restoring the Bureau, sharing liability, removing silos, and making better use of SARs will strengthen our defenses.

Thank you.

[The prepared statement of Mr. Rust follows:]



Statement for the Record

Adam Rust
Consumer Federation of America
For the hearing
"Fighting Fraud on the Front Lines: Challenges and Opportunities for Financial Institutions."
Subcommittee on Financial Institutions
House Financial Services Committee
2120 Rayburn House Office Building
March 5, 2026

Honorable Chair Andy Barr Room 2430
Rayburn House Office Building
Washington, DC 20515

Ranking Member Bill Foster
Rayburn House Office Building Room 2336
Washington, DC 20515

Dear Honorable Chair Barr and Ranking Member Foster:

Thank you for the opportunity to submit this statement and testify before your committee.

The Consumer Federation of America (CFA) is an association of non-profit consumer organizations established in 1968 to advance consumer interests through research, advocacy, and education.

Financial fraud and scams represent one of the most rapidly escalating threats to American consumers and the integrity of our financial system. Today, criminal organizations apply sophisticated scams, evade detection, and adapt their methods to stay ahead of law enforcement. They impersonate government officials to collect fabricated debts, pose as employers directing employees to transfer funds, and exploit personal relationships by masquerading as family members or close friends facing emergencies. They manipulate victims through romance schemes, fraudulent lottery notifications, and targeted extortions. These examples represent only a subset of their tactics, and new ones emerge regularly. While they differ in their methods, they share a common purpose: to compel a victim to send money. No individual is truly insulated from these threats. They affect people from all backgrounds, civilians and servicemembers, old and young, rich and poor, and in every Congressional district.[1]

These are escalating problems demanding attention. The number of fraud reports has increased steadily over the last 25 years. In 2001, the Federal Trade Commission received 325,519 fraud complaints; in 2024, more than 1.8 million; and in 2024, approximately 6.47 million.[2] We know of reports from victims totaling $12.5 billion in losses,[3] but the number is surely greater, as many victims never file a report.

They have increased in part because of converging forces in American life that give criminals more opportunities. Twenty years ago, people did not carry internet-connected mobile devices capable of initiating electronic funds transfers. Most financial arrangements occurred in person rather than over the internet, and bank-fintech partnerships were yet to come. Social media platforms existed, but they were not ubiquitous forums for information sharing. Digital commerce was conducted almost exclusively with network-branded cards, which carried (and continue to carry) fraud protection and institutional scam-prevention technologies. To the extent that our personal data was available online, the scope is only greater now, and constant breaches of private information were still to come. Facebook was exclusively for students until 2005 and did not have a chat function until 2008.[4] All of these forces reinforce each other, creating environments where fraudsters can reach virtually anyone, to the benefit of criminal organizations seeking to steal from people.

The primary law governing consumer fraud protections for electronic funds transfers – the Electronic Funds Transfer Act – was passed almost fifty years ago. It gives consumers rights against unauthorized transfers, but the protection available to victims of scams is at best thin. Transfers authorized by payment

---

[1] Federal Bureau of Investigation. (2025). *Internet Crime Report*. Internet Crime Complaint Center. https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

[2] Federal Trade Commission. (2025). Consumer Sentinel Network Data Book 2024. https://www.ftc.gov/system/files/ftc_gov/pdf/csn-annual-data-book-2024.pdf

[3] Federal Trade Commission. (2025). New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024. https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024

[4] Felix Richter. (2019, February 5). How Facebook grew from 0 to 2.3 billion users in 15 years. World Economic Forum. https://www.weforum.org/stories/2019/02/how-facebook-grew-from-0-to-2-3-billion-users-in-15-years/

apps, wire transfers, digital assets, and bank P2P apps are considered authorized. To the extent scam victims receive relief, it is due to voluntary responses by providers, and not by the force of law.

It is within this context that the Committee convenes today.

The Consumer Financial Protection Bureau (CFPB) fights for consumers who are victims of scams and fraud.

The Consumer Financial Protection Bureau plays a critical role in protecting the financial security of American households from scams. In payment, the CFPB's gambit includes authority for the Electronic Funds Transfer Act (EFTA) and Regulation E. The CFPB can also apply its powers to prohibit unfair, deceptive, and abusive acts and practices. Through consumer response, the CFPB takes action when consumers file complaints.

As recently as a year ago, the CFPB was taking meaningful and increasingly assertive steps to address the crisis of scams. In December 2024, the CFPB filed a lawsuit against Early Warning Systems (EWS), the company behind the Zelle network, along with three of its major bank owners. The lawsuit alleged operational failures that left consumers without adequate protection from scams, resulting in an estimated $870 million in consumer losses.

In January 2025, the CFPB ordered Block, the corporate parent of Cash App, to pay $175 million in relief to harmed consumers and to implement substantive improvements to its fraud-prevention infrastructure. The CFPB found that Block violated the Electronic Funds Transfer Act (EFTA) by failing to investigate unauthorized transactions properly and by having inadequate fraud-detection systems.[5]

These actions sent a clear signal that the CFPB was prepared to hold banks and non-banks accountable when payment companies introduced unsafe products to the market. Moreover, the CFPB had shown that it would apply not just its powers under EFTA, but also those against UDAAPs, to help victims. But the attempts to shutter the CFPB make consumers vulnerable to scams and fraud.

Unfortunately, recent attacks on the CFPB have made consumers vulnerable to scams, prevented the agency from supervising payment apps, and absolved companies of accountability.

In March 2025, the CFPB dropped its lawsuit against EWS, Bank of America, Wells Fargo, and JPMorgan Chase. Furthermore, it did so *with prejudice,* meaning that it cannot be refiled.

In May 2025, Congress passed a resolution disapproving of the CFPB's November 2024 rule (the "payment apps rule") that would have subjected larger participant non-bank payment app and digital wallet products to federal supervision. The payment apps rule would have given the CFPB the authority to monitor the payment apps relied on by tens of millions of households to transfer funds. Incredibly,

[5] Consumer Financial Protection Bureau. (2025, January 16). *CFPB Orders Operator of Cash App to Pay $175 Million and Fix Its Failures on Fraud*. https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-operator-of-cash-app-to-pay-175-million-and-fix-its-failures-on-fraud/

Congress chose to remove a layer of oversight only two months after the Federal Trade Commission released new data showing that fraud-related losses on payment apps had tripled from 2021 to 2024.[6]

Because of the reversal of the payment apps rule, the pressures that prevailed on EWS to address Zelle's risk controls are unlikely to be brought to bear on non-bank payment apps and digital wallets. True, the CFPB retains enforcement authority for any violations of EFTA. But in practice, the new administration has eviscerated the CFPB's supervision and enforcement work. The oversight gap will only grow larger over time, as the volume of payment app transfers increases and new entrants add to the number of now federally unsupervised companies. Payment apps continue to be the subject of many consumer complaints. In the 3rd quarter of 2025, payment app complaints crossed a new threshold. For the first time, payment apps were the leading payment type involved in fraud-related complaints tracked by the FTC.[7]

Congress should restore the CFPB's authority to supervise non-bank payment apps and digital wallets and build on the 2024 rule by adding supervision of transfers involving digital assets.

CFPB funding should be restored to its full level

In the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank), Congress established an important provision allocating up to 12% of the Federal Reserve's earnings to fund the CFPB. Earlier this year, the CFPB's funding cap was reduced to 6.5 percent of the Federal Reserve's 2009 operating expenses, with inflation adjustments. By slashing the agency's budget, Congress has undercut the agency's ability to fulfill its duties.

During this time, the new administration has attempted to illegally shutter the CFPB. New leadership at the CFPB has attempted to conduct massive reduction-in-force (RIF) orders.[8] It has ordered staff to stop work. To the extent that supervision occurs, it is far more limited. Sixty-seven guidances were withdrawn in a single day.[9] The agency has permanently dismissed 22 enforcement actions. As a result, consumers have lost $3.5 billion in restitution that would otherwise have been paid to remedy the harm they experienced at the hands of the offending companies.[10]

Nonetheless, the American people are still approaching the CFPB, seeking a resolution to problems they have encountered with their financial services provider. The volume of complaints has grown every year since the agency's launch. In 2025, consumers filed more than five million complaints.

Unfortunately, the likelihood that a consumer receives relief is declining sharply. Data from the CFPB's complaint database reveals a dramatic and accelerating drop in the rate at which financial institutions are

---

[6] Federal Trade Commission. "All Fraud Reports by Payment Method: Year 2024." Tableau Public website. Fraud Reports, March 7, 2025. https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods.

[7] Federal Trade Commission. "All Fraud Reports by Payment Method: Year 2025." Tableau Public website. Fraud Reports, December 11, 2025. https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods.

[8] Caitlin Mullen. (2025, April 22). CFPB defends analysis behind 90% job cuts |. *Banking Dive*. https://www.bankingdive.com/news/cfpb-layoffs-job-cuts-vought-paoletta-nteu-berman-jackson-appeals-court/746009/

[9] Gabrielle Saulsberry. (2025, May 12). CFPB rescinds 67 pieces of guidance. *Banking Dive*. https://www.bankingdive.com/news/cfpb-rescinds-67-pieces-guidance-vought/747790/

[10] Senator Elizabeth Warren, Ranking Member. (2026). *New Report Finds Trump's Attack on the CFPB Has Cost Americans $19 Billion in One Year Alone*. United States Committee on Banking, Housing, and Urban Affairs. https://www.banking.senate.gov/imo/media/doc/cfpb_year_in_review_report.pdf

providing relief to complainants. The trend suggests that the companies now believe they face little accountability for ignoring customer complaints.

The data reveals a significant shift since 2024. Then, roughly half of all complaints resulted in a positive resolution for consumers, either monetary compensation or the correction of a problem. Beginning in summer 2025, patterns began to change, and positive outcomes became less common. By November 2025, only five percent resulted in relief. By mid-December, the figure fell below 1 percent.[11]

The CFPB has even pulled back on its commitment to help service members. In its initial RIF, the CFPB fired every staff member in the Office of Servicemember Affairs, save for its division leader. However, that staff member had accepted a voluntary retirement. Military and veterans organizations have expressed their strong support for the agency.[12] Indeed, the CFPB has the primary federal authority to supervise and enforce the Military Lending Act. Luckily, the courts stood up for service members, and the cuts were rejected.

Congress should restore the CFPB's funding to the original 12 percent cap as called for in the Dodd-Frank Act.

Unsafe financial products that harm consumers for reasons they cannot prevent are unfair.
The CFPB brought the 2024 lawsuit against EWS because it has EFTA authority for transfers, but the order involved causes of action that violated prohibitions against "unfair, deceptive, or abusive acts or practices (UDAAPs)."[13]

UDAAPs can occur when any covered financial product or service is offered. In an action using UDAAP, the cause(s) of action must meet the three-part unfairness standard: that the failures caused substantial injuries to consumers; consumers could not reasonably avoid the harms, and countervailing benefits to consumers or competition did not outweigh the injury.[14]

Companies should be accountable when they rush dangerous products to market – in any market. According to the CFPB, when EWS introduced Zelle, it designed the network for sending and receiving payment messages; however, it could have incorporated stronger fraud prevention capabilities into the software. For example, EWS could have embedded fraud-detection tools within the system's operating software. If it had done this, the network would have been safer. The CFPB held both the network and its three largest bank participants accountable for offering an unsafe product.

---

[11] Adam Rust. (2025, December 22). Trump's CFPB to Nearly a Million Americans: Goodbye, We Prefer Not To Help You · Consumer Federation of America. *Consumer Federation of America*. https://consumerfed.org/trumps-cfpb-to-nearly-a-million-americans-goodbye-we-prefer-not-to-help-you/

[12] Brief of Military and Veterans Organizations as Amici Curiae in Support of Petitioners, No. 22-448 (Supreme Court of the United States). Retrieved https://www.moaa.org/uploadedfiles/22-448-amicus-brief-of-military-and-veterans-organizations.pdf

[13] Consumer Financial Protection Bureau. (2024). *Consumer Financial Protection Bureau v Early Warning Services, Bank of America, JPMorgan Chase Bank, and Wells Fargo Bank, NA.* [Complaint for Permanent Injunction, Monetary Judgment, Civil Penalty Judgment, and Other Relief]. https://www.consumerfinance.gov/enforcement/actions/early-warning-services-llc-bank-of-america-na-jpmorgan-chase-bank-na-wells-fargo-bank-na/

[14] 12 U.S.C. §§ 5531(a), 5536(a)(1)(B)

The complaint described six ways the network and the three bank defendants failed to prevent, detect, or limit fraud:[15]

- Maintaining inadequate systems for authenticating, verifying, and registering applicants to ensure "bad actors" were excluded from the network. For example, EWS permitted "token flipping," where users could register multiple Zelle tokens (with different phone numbers or email addresses) with a single bank. EWS allowed transfers to accounts whose email addresses or phone numbers (tokens) were not linked to a deposit account before the time of the payment order.
- Not giving consumers enough information about the recipients' identity. When launched, Zelle rules required only that banks indicate the recipient's first name, making it harder for a sender to recognize a problem.
- Failing to share some risk-related information with participating FIs that may have warned them to pause or block transfers. While rules required participants to report when an account was closed due to unauthorized fraud, they did not mandate the sharing of information related to induced fraud.
- Failing to suspend or block bad actors from participating in the network.
- Not requiring timely fraud information-sharing among participating FIs. The CFPB found that while network rules required FIs to report unauthorized frauds promptly, in practice, network participants were allowed to delay reporting until "long after it occurred."
- Failing to ensure participants followed network rules.

The events in this narrative meet the unfairness standard: consumers were harmed ($870 million in losses), they could not have prevented the incident (EWS introduced Zelle without safeguards), and there was no countervailing benefit to consumers or competition.

These shortcomings underscore the need for a governance layer in any payment system. Any network that moves consumer funds must be built with a governance layer that includes fraud detection, risk management, and accountability mechanisms. EWS launched Zelle without one, and as a result, account holders lost hundreds of millions of dollars.

Supervision and enforcement prompt companies to make their services safer.

Enforcement actions of the kind brought against EWS require years of investigation, development of legal theories, and ongoing engagement. It is therefore significant that Zelle introduced Zelle Risk Insights (ZRI) in the summer of 2023, during the period when the CFPB's scrutiny of the network was advancing. From a regulatory lens, this outcome is not incidental. It reflects the direct relationship between unsafe product design and unfair consumer outcomes. The Zelle experience demonstrates that supervision and enforcement are not bureaucratic formalities. They are the forces that compel companies to build safer products and bear responsibility when they do not.

---

[15] Consumer Financial Protection Bureau. (2024). CFPB v. Early Warning Services, LLC; Bank of America, N.A.; JPMorgan Chase, NA.; and Wells Fargo Bank, N.A. [Complaint for Permanent Injunction, Monetary Judgment, Civil Penalty Judgment and Other Relief]. https://files.consumerfinance.gov/f/documents/cfpb_Zelle-Complaint_2024-12.pdf

ZRI advanced Zelle from a simple messaging system to a risk-sensitive platform. For the first time, network rules held participating banks accountable for using fraud-detection information. It created systems for flagging high-risk accounts, additional identity-verification overlays, and a new impostor-scam refund system.

These are all positive changes – but they cannot be evaluated in isolation from the regulatory context in which they were made. The evidence strongly suggests that these improvements were a direct response to the CFPB's supervision and enforcement work, rather than to a voluntary industry initiative.

If the CFPB's investigation into Zelle drove EWS to make reforms, it would not be the first instance where enforcement led to better outcomes for consumers in the broader market. During the last administration, the CFPB and prudential regulators cracked down on aggressive bank overdraft and non-sufficient funds (NSF) fee harvesting. The CFPB completed enforcement actions against banks in 2017, 2020, 2022, 2023, and 2025.[16] During this time, many banks began to reform their policies. By 2024, the CFPB's work had led to proactive savings of $4 billion per year in overdraft and NSF fees that might have otherwise been paid.

For policymakers, developments in overdraft and faster payment markets that arose from investigations should demonstrate why the goal of a safe financial ecosystem hinges on a strong financial regulator to oversee markets, conduct investigations, and enforce consumer protection.

Congress should pass legislation restoring the CFPB's ability to supervise non-bank payment apps and digital wallets.

Crypto kiosks are a dangerous vector for scams.

There are now over 30,000 crypto kiosks across the United States. Without state intervention, these kiosks lack consumer protection. In 2024, the FBI received almost 11,000 complaints about crypto kiosks, resulting in nearly $250 million in losses. Adults over the age of 60 suffered approximately 85 percent of those losses.[17] Losses increased tenfold between 2020 and 2023.[18] Since a very high share of scam losses are never reported, these numbers reflect only a fraction of total harm.[19] CFA supports legislation to curb the abusive practices of crypto ATMs:

- Set mandatory daily transaction limits
- Limit fees to $5 per transaction of 15 percent, whichever is lower.
- Require paper receipts for all transactions
- Post clear, visible scam warnings at every kiosk
- Require mandatory holds on transfers to allow time to reverse fraudulent or coerced payments.

---

[16] Consumer Financial Protection Bureau. (2024, September 17). CFPB Takes Action to Stop Banks from Harvesting Overdraft Fees Without Consumers' Consent. https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-to-stop-banks-from-harvesting-overdraft-fees-without-consumers-consent/

[17] AARP. (2026, January 28). AARP Backs Legislative Action to Stop Crypto Kiosk Scams. https://www.aarp.org/states/washington/aarp-backs-legislative-action-to-stop-crypto-kiosk-scams/

[18] Federal Trade Commission. (2024). Bitcoin ATMs: A payment portal for scammers [Data Spotlight]. https://www.ftc.gov/system/files/ftc_gov/pdf/bitcoin_atms_spotlight.pdf

[19] Anderson, K. B. (2021). To Whom Do Victims of Mass-Market Consumer Fraud Complain? (SSRN Scholarly Paper No. 3852323). Social Science Research Network. https://doi.org/10.2139/ssrn.3852323

- Subject all kiosk operators to state licensure.

By early 2026, seventeen states had passed laws regulating crypto kiosks. In announcing a lawsuit against a crypto kiosk operator, District of Columbia Attorney General Brian L. Schwalb revealed that the agency's investigation found 93 percent of the company's transactions were fraudulent.[20]

These measures will protect consumers from scams. They will also suppress the use of crypto kiosks for illicit finance.

Policymakers should strengthen the connections between consumer protection agencies and those fighting illicit finance.

A critical gap exists in how Bank Secrecy Act (BSA) enforcement has traditionally been conceptualized in light of emerging large-scale international scam operations. Even when regulators identify failures to prevent illicit finance, the resulting enforcement actions largely overlook the direct harms experienced by consumer victims. BSA compliance has focused on stopping money laundering, terrorist financing, human trafficking, drug sales, and international government corruption. No one argues that those are essential purposes. When illicit finance flourishes, it harms people in tragic ways.

But the organizations investigated for illicit financial crimes have now opened a new line of business: scamming regular people. In several Southeast Asian countries, scams fund a large share of national economic activity.[21] There is a consistent overlap in which scams are one component of criminal operational portfolios.[22]

FinCEN has itself signaled that this broader view is warranted. In its 2021 Anti-Money Laundering and Countering the Finance of Terrorism (AML/CFT) National Priorities report, FinCEN listed fraud as one of eight national priorities. In listing fraud, it made clear that the term encompassed common scam tactics: impostor schemes, confidence fraud, employment scams, and related methods.

> *"Increasingly, fraud schemes are internet-enabled, such as romance scams, synthetic identity fraud, and other forms of identity theft. Proceeds from fraudulent activities may be laundered through a variety of methods, including transfers through accounts of offshore legal entities, accounts controlled by cyber actors, and money mules."*[23]

And, critically, it attributed the work to the same organized criminal networks engaged in other transnational crimes. The activities FinCEN identified, and the flow of funds associated with them to US

---

[20] Attorney General Brian L. Schwalb. (2025, September 8). Attorney General Schwalb Sues Crypto ATM Operator for Financially Exploiting District Residents. https://oag.dc.gov/release/attorney-general-schwalb-sues-crypto-atm-operator

[21] McClure, T. (2025, December 2). Age of the 'scam state': How an illicit, multibillion-dollar industry has taken root in south-east Asia. The Guardian. https://www.theguardian.com/technology/2025/dec/02/scam-state-multi-billion-dollar-industry-south-east-asia

[22] Sims, J. (2025). Policies and Patterns: State-Abetted Transnational Crime in Cambodia as a Global Security Threat. Human Research Consultancy. https://cdn.prod.website-files.com/662f5d242a3e7860ebefde4f/68264cff356caba111f2db1e_Policies%

[23] FinCEN. (2021, June 30). Anti-Money Laundering and Countering the Financing of Terrorism National Priorities. https://www.fincen.gov/system/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf

depositories and money transmitters, are precisely the actions that call for closer ties between consumer protection agencies and those charged with stopping illicit finance.

Scams targeting the elderly underscore the need for solutions that protect consumers from such scams and combat illicit financial crime.

FinCEN has stated that SARs can be helpful in understanding how fraud affects consumers. For example, in 2011, it issued an advisory to financial institutions, noting that their information could help combat elder financial fraud. It specifically noted that financial institutions can communicate with federal and state regulators to support fraud prevention efforts.[24]

Seniors are a primary target of scammers. All things being equal, they are more likely to have savings, and some will suffer from cognitive impairments, making them more vulnerable to exploitation. In response, FinCEN has prioritized addressing elderly financial exploitation (EFE). The findings detailed in its recurring Financial Trend Analysis reports show why it is imperative to eliminate boundaries between consumer protection agencies and agencies charged with preventing illicit financial crime.

Many scam incidents do not lead to SAR filings: FinCEN estimated that in 2017, EFE-related SARs filed accounted for less than 2 percent of actual EFE incidents.21 Disturbingly, the number of EFE-related SARs has increased every year, even though estimates suggest that only a small minority of EFEs result in a SAR filing.[25]

Scams are sometimes the first step in subsequent money laundering activities. Often, funds received through scams are transferred to other accounts via money mules.[26] These are funnel accounts.

Preventing account takeover is a critical challenge. FinCEN reported that most elder scam-related filings referenced account takeovers.[27]

Sharing is inconsistent. The likelihood that an EFE results in a SAR appears to vary widely across institutions. In the 12 months ending in June 2023, two banks made 33 percent of all SAR filings.[28] Fewer than 5,000 financial institutions filed EFE-related SARs during that period. Given that this number includes money service businesses and other covered non-banks, it is likely that thousands of depository institutions did not file any EFE-related SARs.

---

[24] Advisory to Financial Institutions on Filing Suspicious Activity Reports Regarding Elder Financial Exploitation (FinCEN Advisory No. FIN-2011-A003). (2011). https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2011-a003

[25] FinCEN. (2022). Advisory on Elder Financial Exploitation (FinCEN Advisory No. FIN-2022-A022). https://www.fincen.gov/system/files/advisory/2022-06-15/FinCEN%20Advisory%20Elder%20Financial%20Exploitation%20FINAL%20508.pdf

[26] FinCEN. (2024). Elder Financial Exploitation: Threat Pattern and Trend Information, June 2022 to June 2023 [Financial Trend Analysis]. https://www.fincen.gov/system/files/shared/FTA_Elder_Financial_Exploitation_508Final.pdf

[27] FinCEN. (2019). Elders Face Increased Financial Threat from Domestic and Foreign Actors [Financial Trend Analysis]. https://www.fincen.gov/system/files/shared/FinCEN%20Financial%20Trend%20Analysis%20Elders_FINAL%20508.pdf

[28] Ibid

According to FinCEN, most EFEs involved transfers made through money service businesses (MSBs) to scammers operating from Africa and Asia. SARs involving EFEs filed by depositories were much less likely to indicate a foreign recipient, but 47 percent could not identify the location.[29]

The fraud/scam distinction in EFTA and Reg E must be reevaluated

The liability framework for scams requires fundamental reform. At the heart of the problem is an outdated legal distinction embedded in the Electronic Fund Transfer Act (EFTA) and its implementing rule, Regulation E. Under current law, consumers are protected when funds are taken from their accounts without their consent. However, consumers receive no equivalent protection when they are deceived or coerced into initiating a transfer themselves. Because the account holder technically authorized the payment, these transactions are classified as "scams" and fall outside existing consumer protections.

This distinction, once perhaps administratively coherent, has become increasingly disconnected from the reality of modern criminal tactics. Sophisticated fraud schemes routinely manipulate victims into authorizing payments under false pretenses. The resulting transfers are "authorized" only in form.

The methods by which criminals conduct fraud and scams have evolved since the 1970s. When the EFTA was passed in 1978, virtually all electronic funds theft involved stolen automated teller machine (ATM) cards or compromised personal identification numbers (PINs). At this time, almost all losses were due to unauthorized transfers. When the Federal Reserve issued Regulation E to implement EFTA in 1979, it defined an unauthorized payment as one initiated by someone other than the consumer. They focused on the critical risks of the time – stolen PINs and lost or stolen ATM cards.

In 1981, the Federal Reserve introduced a new wrinkle: transfers initiated by the account holder are considered unauthorized payments if the consumer is "conned or forced to furnish another person with an access device for use in an ATM."[30] A few months later, the commentary was updated to state that when a consumer is "induced by fraud to furnish another person with an access device" to make an ATM withdrawal, the payment is also unauthorized. Fed staff reasoned that criminals might force people to withdraw funds at ATMs. In 1983, this example was provided in a staff commentary.[31]

These commentaries are the first instances in which regulators acknowledged that criminals might coerce consumers to initiate an EFT. Congress's conclusion in 1981—that electronic funds transfers made through inducement are also unauthorized—shows that today's inducement schemes also deserve reclassification as unauthorized payments.

Any durable legislative or regulatory solution must eliminate this distinction and extend meaningful protections to consumers who are induced through deception or coercion to send funds, regardless of whether the account holder technically initiated the payment.

---

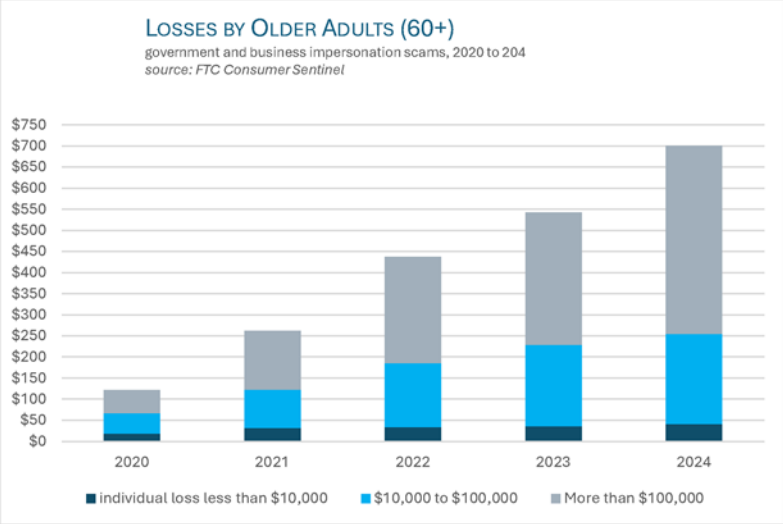
[29] Ibid

[30] Technical Amendments and Official Staff Commentary Update, 48 Fed. Reg. 4667, 4668 (Feb. 2, 1983).

[31] Official Staff Commentary Update, 50 Fed. Reg. 13180, 13181 (April 3, 1985) ("Q 2-28: Unauthorized transfers – forced initiation. A consumer is forced by a robber (at gunpoint, for example) to withdraw cash at an ATM. Do the liability limits for unauthorized transfers apply? A. Yes. The transfer is unauthorized for purposes of Regulation E. Under these circumstances, the actions of the robber are tantamount to the use of a stolen access device.").

Scams harm some of our most vulnerable populations

The rise in scams disproportionately affects seniors. High-loss scams start with similar narratives: someone is using your account, your information is being used to commit crimes, or there is a security problem with your computer. They end tragically. According to a recent FTC report, the number of older adults who lost more than $10,000 in a scam increased fourfold from 2020 to 2024. Losses of more than $100,000 increased sevenfold, and total sums lost increased eightfold.[32]



The criminal coerces the victim to authorize a payment, a significant problem for existing laws, as authorized funds transfers fall outside of EFTA protections.

Owing to their use of smartphones, young people are more likely to fall prey to sextortion schemes. The National Center for Missing & Exploited Children (NCMED) said that an overwhelming share of cases are initiated online, most often through Instagram and Snapchat. The number of reports jumped dramatically during the pandemic. NCMEC says it receives more than 1,000 reports per week.[33]

As well, servicemembers are vulnerable to scams. During a permanent change of duty station, service members must find new housing. While junior personnel may be relocated to a new barracks room, others will need to secure a private residence. When relocating, service members rely on payment apps at rates

---

[32] Division of Consumer Response and Operations Staff. (2025). False alarm, real scam: How scammers are stealing older adults' life savings. Federal Trade Commission. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2025/08/false-alarm-real-scam-how-scammers-are-stealing-older-adults-life-savings

[33] National Center for Missing and Exploited Children & Thorn. (2024). *Trends in Financial Sextortion: An investigation of sextortion reports in NCMEC CyberTipline data*. https://www.thorn.org/research/library/financial-sextortion/

far more frequently than civilians. As a result, criminals are now targeting service member accounts. To make matters worse, some payment apps limit customer service hours, making it harder for servicemembers stationed overseas in different time zones to resolve problems. The number of complaints filed by servicemembers about payment apps has increased steadily in the last few years, and many have been related to fraud and scams using payment apps.[34] Service members report being unable to access funds when their accounts are frozen.[35]

Expand EFTA to include protections for consumers who are scammed into sending wire transfers.
While wires are the preferred payment rail for corporations making large-value transfers, they are still used by consumers on occasion. Moreover, wires are often used in some of the largest scams perpetrated against regular people, such as investment scams resulting in losses of hundreds of thousands of dollars.

Wire transfers are classified as out of scope of EFTA.[36] Instead, the Uniform Commercial Code Article 4A governs wire transfers. Article 4a absolves banks of liability as long as they followed "commercially reasonable security procedures," even if the sending customer was scammed.

Through staff commentaries, the Federal Reserve has concluded that EFTA and its implementing regulations do not apply to funds transferred through Fedwire. However, in 2024, the CFPB filed a statement of interest in New York v. Citibank, N.A., making the point that EFTA should apply to wires sent by consumers.

Share liability between sending and receiving financial institutions
Policymakers must apply liability to the "bank of the criminal" and the "payment app of the criminal."

Regardless of the narrative employed and the method used to contact the victim, scammers must have a place to receive funds. While cryptocurrency and Bitcoin ATMs are emerging as popular tools for this purpose, criminals still need to use depositories and payment apps. As long as consumers place their funds in either, scammers will need accounts inside them.
Scammers can gain access to an account in one of three ways: by applying for one directly, typically using a synthetic identity; by taking over an account; or by using a money mule to move funds on their behalf. In each case, the FI is the first line of defense against scams. Once they have gained a foothold, scammers use the account to receive proceeds from scams and then move those dollars to another location.

Most often, they search for and target FIs with weak fraud detection systems. For example, they may see that a bank has only recently introduced online or app-based banking services. Criminals share information, so they may quickly flood an FI with applications after the first successful compromise. The

---

[34] *CFPB Report Identifies Issues with Increased Servicemember Use of Digital Payment Apps*. (2023, June 20). Consumer Financial Protection Bureau. https://www.consumerfinance.gov/about-us/newsroom/cfpb-report-identifies-issues-with-increased-servicemember-use-of-digital-payment-apps/

[35] Consumer Financial Protection Bureau. (2022, November 11). *Consumer Complaint Database* [Consumer Complaint, Seam]. https://www.consumerfinance.gov/data-research/consumer-complaints/search/detail/6190058

[36] 15 U.S.C. § 1693a(7)(B)

FI's failure to reject fraudulent applications, prevent account takeovers, and monitor accounts for suspicious activity is not a peripheral compliance lapse. It is the condition that makes a scam possible. Weak customer due diligence (CDD) controls directly enable consumer harm.

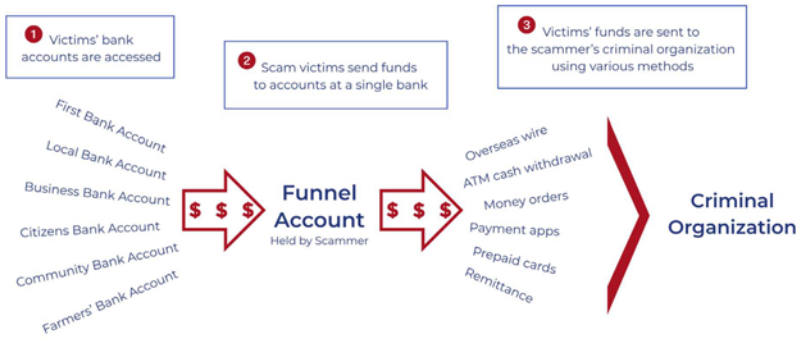
The dynamic places receiving FIs at a critical place in the scam chain. The "FI of the criminal" has a unique line of sight into suspicious behavior. They should know who holds the account and its declared uses. As such, they are better situated to see suspicious activity than senders. The tools required to conduct these reviews need not be developed in-house. They are widely available through contracts with third-party vendors.

The Funnel Account: How A Single Bank with Poor Scam Prevention Puts Everyone at Risk of Scams

A key problem is the "funnel account." Criminals use funnel accounts to receive money. Funnel accounts affect transfers across all faster payments, checks, wires, and Automated Clearing House (ACH) transfers. An FDIC-insured account can serve as a funnel account, but a non-bank P2P wallet can also fulfill this purpose. A single funnel account can be used to receive numerous fraudulent transfers, serving as the hub to accept scam funds from multiple sending banks.

Often, funds are deposited into funnel accounts and then withdrawn as soon as they settle.

This problem is only getting worse. The number of SARs identifying a funnel account has increased fourfold since 2020.[37] In the first six months of 2025, nearly 8 percent of bank account applications were made using synthetic identities.[38] With the rise of online banking, the share of applications made online has increased. New account fraud is enabled by stolen identities and made easier by artificial intelligence.[39]



[37] David Maimon. (2025, October 21). Fraud In America 2025: The Laundering Network Exploiting Banks. Forbes. https://www.forbes.com/sites/davidmaimon/2025/10/21/fraud-in-america-2025-the-laundering-network-exploiting-banks/

[38] Sentilink. (2025). The Sentilink Fraud Report: Identity Fraud Rates and Trends (No. H1 2025). https://insight.sentilink.com/hubfs/The_SentiLink_Fraud_Report_H1_2025.pdf

[39] Fraud.com (2023, April 5). 5 reasons behind the increase in digital banking fraud. https://www.fraud.com/post/increase-in-digital-banking-fraud

Poor fraud prevention by even a small number of RDFIs can lead to significant fraud. When criminals exploit a handful of vulnerable accounts to receive and then launder funds, they can create a small network of accounts to funnel funds.

To force investment across the entire payment ecosystem, incentives should be put in place to increase financial institutions' motives to identify and pause suspicious activity.

Policy approaches that call for shared liability are sensible and would be effective. Returning to the case of ZRI, one of the critical elements of its update was the requirement that participating institutions contribute to and use shared fraud-detection information.

In fact, it is not unreasonable to see a future in which the distinguishing features of payment channels are security, speed, and cost. Chartered financial institutions and state-licensed money transmitters will face new competition from blockchain-based settlement, driven forward by agentic AI shopping. The cost of routing a transaction through a Layer 2 blockchain could be very low, nearly immediate on a 24-7 basis, and also very risky. At the moment, it appears that most bank-routed transactions will settle more slowly and at a greater cost.

Shared liability will place greater scrutiny on KYC-lite practices, including those involving bank-fintech partnerships.

All financial institutions face a tension in attracting new accounts. The imperative to grow, along with the desire to see returns on marketing costs, makes it imperative to minimize "friction" in processes for opening new deposit and loan accounts. Each new data point in an application form inevitably leads to more abandonments and fewer completions.[40] Compliance risks push in the opposite direction, requiring FIs to collect more information to verify customer identity. Together, these pressures act in conflict. Too often, some FIs succumb to the temptation to perform "KYC-lite."

This tension is particularly acute in the fintech sector. In the last six years, prudential regulators have issued enforcement actions and settlements with a high share of partner banks.[41] In 2023, enforcement actions were issued to Cross River Bank, Metropolitan Commercial Bank, Vast Bank, B2 Bank, First Fed Bank, and Choice Financial Group. Blue Ridge Bank, Lineage Bank, Sutton Bank, Piermont Bank, and Evolve Bank & Trust received orders in 2024.[42] Most involved AML compliance failures.

For a number of reasons, fintech accounts are in the crosshairs of criminals. Not least, they operate exclusively online and are frequently very new. But fintech companies also bring healthy risk appetites to the table. These companies, and especially early-stage firms operating under pressure from impatient

---

[40] Terry Badger. (2023, February 10). Fixing the top of the digital funnel. BAI. https://www.bai.org/banking-strategies/fixing-the-top-of-the-digital-funnel/

[41] S&P Global. (2024, January 23). Small group of banking-as-a-service banks logs big number of enforcement actions. https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/small-group-of-banking-as-a-service-banks-logs-big-number-of-enforcement-actions-80067110

[42] Son, H. (2024, July 2). How thousands of Americans got caught in fintech's false promise and lost access to bank accounts. CNBC. https://www.cnbc.com/2024/07/02/synapse-fintech-fdic-false-promise.html

investors, have strong financial incentives to minimize friction. In turn, partner banks face corresponding incentives. To attract business from fintechs, they may feel competitive pressure with competitor partner banks to offer streamlined compliance standards.

Federal interagency guidance on third-party risk is clear and unambiguous: banks are responsible to ensure their non-bank partners follow the rules.[43]

Unfortunately, too large a share of bank activity now occurs outside the banking perimeter. While some banks have BaaS programs inside their bank holding companies, other banking-as-a-service (BaaS) firms operate outside prudential supervision. Independent banking-as-a-service (BaaS) companies must face greater regulatory scrutiny.

The failures at Synapse, an independent BaaS firm, illustrate the problem. Working in conjunction with a roster of consumer and small business fintechs and four bank partners, Synapse failed to properly ledger consumer account balances. Following the company's bankruptcy, a court-appointed trustee estimated that between $65 and $96 million in customer funds were unaccounted for, affecting more than 100,000 consumers.[44] These funds were owed to consumers at a variety of fintech apps, but neither Synapse nor its bank partners could ascertain the exact amounts due to each depositor.

Evolve Bank & Trust was also central to the failures at Synapse. A partner bank to fintechs, Evolve was recently found to have permitted scores of accounts to be opened from a single Wyoming address by applicants with IP addresses in foreign countries, including some on the Office of Foreign Assets Control (OFAC) list.

Evolve approved these accounts through its partnership with Mercury, a fintech company serving businesses. The document displays the operational capabilities of the accounts at the time of ledger publication ("permission"), including the phone number prefix and country code of the device used to open the account, the address of record for the account (Street), and the current balance (Deposit US balance). Send and receive accounts are fully capable of making fund transfers. Locked accounts are open but cannot send or receive funds. While many are now closed, they were all active at one point, and all still had balances when this ledger was published in a court filing. The same hearing found evidence that Evolve had failed to fulfill the Office of Foreign Asset Control's requirements for seven years.

Criminals have used fintech accounts issued by Evolve for other third-party fintech programs. For example, a Nigerian group used Juno debit card accounts to receive funds from business email compromise scams, tax scams, and romance scams.[45]

---

[43] Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, & Board of Governors of the Federal Reserve System. (2023, June 6). Interagency Guidance on Third-Party Relationships: Risk Management. https://www.fdic.gov/news/

[44] Penny Crosman. (2025, August 8). CFPB to hold Synapse responsible for missing customer funds. American Banker. https://www.americanbanker.com/news/cfpb-to-hold-synapse-responsible-for-missing-customer-funds

[45] Ibid

The prudential regulators should apply their authority under the Bank Service Company Act to supervise independent BaaS firms. Some contend that this power is underutilized.[46] The Synapse event should add urgency among prudential regulators to strengthen its use.

Distribute funds from BSA enforcement to provide remedies for victims of scams.

There is a victim – or perhaps many victims – behind each scam. When considering the reasons this is possible, the significance of RDFIs is especially relevant, given that criminals scour the internet to find banks with lax CDD systems. In underground markets, criminals seek access to stolen accounts that are most likely to evade suspicion, such as those that have been active for over a year or that their legitimate owners have used to make larger fund transfers. Sometimes, criminals open accounts, groom them for months or years by making innocuous deposits and withdrawals to mimic legal use, and then sell them at a premium on the dark web. Some even post pictures of account histories to enhance the desirability of for-sale accounts.[47]

Those accounts may have been used to transfer funds among criminals involved in various illicit money-laundering activities. Some transfers will be used to move money between criminals to operate their illegal enterprises. However, some accounts opened by criminals will be used to perpetrate imposter scams, investment scams, or other scams. The same dynamic applies to accounts that have been taken over: some are used for money laundering, while others are used to receive transfers from fraudulent activity. The latter outcome highlights the importance of incorporating consumer protection components into BSA supervision. When consumers are induced to send funds to a scammer, activities that regulators review for BSA compliance are relevant.

EFTA protects consumers when funds are lost due to unauthorized transfers but leaves victims without recourse if they authorize the transfers. Practically speaking, the current regulatory framework prevents scam victims from receiving relief. Changing enforcement to give victims a share of bank penalties will sidestep one hurdle posed by outdated regulatory distinctions between fraud and scams.[48] While it will not have uniform effects – as it will only aid victims of the most significant failures – it moves in the right direction.

When the UK Payment System Regulator implemented a new code requiring shared liability for scams, the number of complaints fell.

Accountability is essential to making our payment systems safer. This principle must be applied across the payment journey. Currently, consumer protection focuses primarily on the financial institution that sends funds. Bank and non-bank senders must have responsibility, but so should the institutions on the other side of the payment as well.

---

[46] Kiah Lau Haslett. (2025, January 9). Regulatory Exams of Third-Parties Are Hard to Find, Sometimes "Stale," Critics Say. FinXTech. https://finxtech.com/regulatory-exams-of-third-parties-are-hard-to-find-sometimes-stale-critics-say

[47] Maimon, D. (2025, February 26). Investigating Stolen and Forged Treasury Checks. https://resources.sentilink.com/blog/stolen-and-forged-treasury-checks

[48] See for example, FedNow. (n.d.). FraudClassifier. https://explore.fednow.org/resources/fraud-classifier.pdf

Other countries have moved forward with updating protections against induced fraud. In October 2024, the United Kingdom's (UK) Payment Systems Regulator implemented the Contingent Reimbursement Model to hold banks and building societies accountable when criminals trick account holders into sending funds. Most cases result in reimbursements under a framework where Originating Depository Financial Institutions (ODFIs) and Receiving Depository Financial Institutions (RDFIs) share liability.[49]

The onset of this new policy has been a success. Notably, it did not provoke a surge in unjustified fraud claims by people posing as victims. In 2023, UK consumers filed 56,000 scam ("authorized push payment") per quarter on average. In the first three months after the CRM's introduction, the number of scam complaints fell by almost 18 percent, to 46,000.[50] The UK's latest report, covering the first two quarters of 2025, continues to show a decline in confirmed cases.[51]

Pass legislation to provide protection for victims of scams, expand liability to receiving institutions, and take steps to ensure the CFPB can hold financial companies accountable.

Just as it is important to involve government across agencies, it is also important to compel action from financial institutions across the payment journey.

At each stage of the payment journey, institutions face challenges in preventing scams. For sending-side institutions, it may be challenging to overcome an account holder's desire to send funds to a scammer. For a receiving institution, deploying the technology needed to thwart application and account takeovers (ATOs) by criminals will require vigilance and expense. The networks that serve as connectors, which may also control directories, may not understand activities occurring outside of their systems.

Nonetheless, all of these actors can play an important role in sharing information and flagging suspicious activity. These facts are relevant for depositories and non-banks alike.

For this reason, it would be a critical error to absolve any institution of responsibility for a transfer that results in a scam event. Proposals to exempt depositories or non-banks from liability, on either side of a payment order, will disincentivize investment in scam prevention.

For this reason, CFA supports the *Protecting Consumers from Payment Scams Act*. This act will ensure that losses resulting from fraudulent inducement will receive the same level of protection as funds lost from an unauthorized electronic transfer.

Additionally, the Act wisely shares liability between sending and receiving institutions. In doing so, it follows the lead from the United Kingdom, where the introduction of shared liability led to fewer scams.

---

[49] UK Payment Systems Regulator. "Fighting Authorised Push Payment Fraud: A New Reimbursement Requirement." Policy Statement. Response to Consultation, June 2023. https://www.psr.org.uk/media/iolpbw0u/ps23-3-app-fraud-reimbursement-policy-statement-final-june-2023.pdf.

[50] David Geale. (2025). The story so far: A snapshot of what we've seen since our APP scams reimbursement requirement went live [News and Updates Thought Pieces]. UK Payment Systems Regulator. https://www.psr.org.uk/news-and-updates/thought-pieces/thought-pieces/the-story-so-far-a-snapshot-of-what-we-ve-seen-since-our-app-scams-reimbursement-requirement-went-live/

[51] UK Finance. (2025). Half-Year Fraud Report 2025. https://www.ukfinance.org.uk/system/files/2025-10/Half%20Year%20Fraud%20Report%202025_0.pdf

And further, the Act expands protections for consumers who lose money to scams in which they agree to wire funds. Some banks have now programmed their apps to process wire transfers, and at a discount compared to ordering a wire at a branch. These policies contradict depositories' claims that they strive to prevent their customers from paying criminals in scams.

Also, the Act includes in the definition of an "error" the mistakes made by consumer senders when they are tricked by a criminal. This step will ensure that consumers can seek resolution and recover funds through established processes for unauthorized transfers.

Lastly, to ensure that regulators have the authority they need to address current and future challenges, the Act empowers the CFPB to issue new rules to enforce the Act's provisions.

Social media platforms and telecoms are weak points in systemic defense against scams.
A significant share of scam activity originates from social media platforms.[52] Many scammers contact people through their smartphones. Both systems connect directly to the payment system. Meta has projected that over 10 percent of its 2024 sales revenue came from scammers who purchased ads to attract victims or sell false goods.[53]

Some countries have passed laws holding telecommunications companies and social media platforms accountable for scams conducted on their platforms.

For the moment, methods to address these scam gateways are voluntary and not consistent. JPMorgan Chase has introduced a system that warns account holders when it detects that a Zelle purchase request originated from a social media channel.[54] However, Chase is an exception.

Policymakers should revise rules that protect platforms from scam activity.

Moreover, it appears that sharing liability had beneficial effects on the resilience of the payment ecosystem as a whole. Elsewhere, shared liability policies have gone further to hold other actors involved in the chain of scams responsible. In Singapore, telcos share some liability in cases where their breaches result in fraud losses.[55] In Australia, financial institutions have liability, but accountability has also been extended to telcos and digital platforms. Telcos must block SMS messages with phishing links, monitor their systems for suspicious activities, and conduct investigations to block scam calls. Digital platforms must enhance identity verification for new accounts, freeze suspected scam accounts, prevent scammers from advertising, and remove content when necessary.[56]

In the United States, the bipartisan *Safeguarding Consumers from Advertising Misconduct Act* would hold social media platforms accountable to apply some of the same policies to digital platforms as those

---

[52] Au-Yeung, J. H. and A. (2025, May 15). Meta Battles an 'Epidemic of Scams' as Criminals Flood Instagram and Facebook. Wall Street Journal. https://www.wsj.com/tech/meta-fraud-facebook-instagram-813363c8

[53] Vanian, J. (2025, November 6). Meta reportedly projected 10% of 2024 sales came from scam, fraud ads. CNBC. https://www.cnbc.com/2025/11/06/meta-reportedly-projected-10percent-of-2024-sales-came-from-scam-fraud-ads.html

[54] Chase. (n.d.). Help Protect Yourself From Social Media Scams. Privacy and Security. Retrieved March 1, 2026, from https://www.chase.com/digital/resources/privacy-security/security/social-media-scams

[55] Neira Jones. (n.d.). No Weak Links: The Case for Shared Liability in Fraud and Scam Prevention. BioCatch. Retrieved March 1, 2026, from https://www.biocatch.com/blog/case-for-shared-liability-fraud-prevention

[56] Australian Government Treasury. (2025). Scams Prevention Framework – Protecting Australians from scams. https://treasury.gov.au/sites/default/files/2025-01/p2025-623966.pdf

already adopted in Australia. This law would dramatically strengthen defenses against purchase scams. This Act is a step in the right direction, but financial institutions and consumers need stronger action from Congress.

To increase safety and enable faster payments, regulators should update EFAA to allow receiving FIs to delay account crediting when they detect suspicious activity.

The virtue of real-time gross settlement is also the source of its risk. Because of speed and irrevocability, a faster payment service provides an attractive opportunity to a fraudster. While most other payment methods can be canceled, a faster payment is completed in seconds, and the payee may withdraw it as soon as it is received.[57] Once a consumer discovers they sent the funds to the wrong recipient, it is too late to cancel the order. The scammer's financial institution will have accepted the funds and credited them to the account holder's account. The account holder may even have transferred them to another account at a different financial institution. If funds settled at the speed of a batched ACH transfer—a same-day or the traditional multi-day version—the same vulnerability would not exist because there would be time for a payment order to be canceled.

Effective solutions can be applied to improve defenses. With an application programming interface (API) call, a sending bank can request the receiving bank to check if the receiving account has any of the suspicious factors listed earlier. These "accept/reject" requests are standard technology now. In almost all cases, the time between the request and the response is less than five seconds. Usually, response times are under 1 second.

They can also create analytics to flag suspicious transfers – even if the account is new. For example, if the note in a payment memo line reads "for a puppy," there is a logical reason to reject the transfer. By some accounts, fake puppy scams make up almost one-fourth of all online purchase scams.[58] Similarly, if information gleaned through an application suggests that an account will only be funded twice per month and solely through a direct deposit, it should raise flags when it immediately begins to receive many non-payroll deposits. These are practical, empirically-proven, common-sense approaches.

But in cases where near-real-time analytics flag concerns about scams or fraud, the FI needs to be able to delay account crediting.

To further enhance the ability for FIs to apply their fraud detection systems to help scam victims, the Expedited Funds Availability Act and Regulation CC should be updated to specify that FIs can delay crediting an account when they see suspicious activity.

This clarity would not alter consumers' important rights to challenge account freezes or closures. A consumer should be able to contest a bank's decision to freeze or close their account. When a consumer attempts to access the funds but is denied access, the action should be treated as an error. With that protection, a consumer would receive their necessary error-resolution rights, and the bank would be held

---

[57] Federal Reserve. "Fraud and Instant Payments: The Basics." *Instant Payments Education* (blog), 2024. https://www.frbservices.org/financial-services/fednow/instant-payments-education/fraud-and-instant-payments-the-basics.html.

[58] Better Business Bureau. "BBB Study Update: Average Losses in Puppy Scams Rising, Even as Cases Fall." *Latest News* (blog), December 6, 2022. https://www.bbb.org/article/investigations/27895-bbb-study-update-average-losses-in-puppy-scams-rising-even-as-cases-fall. As an aside, French bulldogs, Yorkies, and Dachshunds are especially risky, leading to almost one-third of puppy scams.

to the investigation standards set out in the EFTA.[59] Once the consumer filed a complaint with the bank about a denied transaction, the institution would have to investigate the payment, and if it could not provide a resolution within 10 days, release the frozen funds or reopen the closed account. In essence, it is possible to balance consumer protections with priorities for scam detection.

As key gatekeepers in the exchange of fraud information, faster payment networks such as Zelle must play a role in identifying risky RDFIs. If necessary, they should force worst-practice banks off their systems.

Giving this flexibility to receiving FIs would advance the adoption of faster payments. While many depositories now participate in a faster payments system, many are "receive-only." Institutions choose not to send funds because of a perceived risk that some recipients lack adequate safeguards to detect scam activity.[60] Those receive-only FIs believe that sending an irrevocable real-time payment could put their customers at risk of scams.

Digital identification systems must observe critical privacy safeguards.

Proposed bipartisan legislation would provide support for states to consider plans for mobile digital identification. By creating a tokenized system for data sharing with strong user-determined permissioning, customers and their FIs would have a powerful tool to verify the identities of recipients of fund transfers.

Fundamentally, any system for tokenizing digital identification must also protect consumers from government surveillance. The use of such a tool must be at the consumer's discretion, not conditioned by other factors, and revocable. There are genuine concerns about "phone home" capabilities embedded in digital state-issued identification that would undermine personal privacy.[61] Unfortunately, the federal government is currently instituting practices that compromise consumer privacy rights to a degree never before seen. For this reason, it makes sense to address aggressive privacy invasions by federal law enforcement first, before operationalizing government-issued digital identification. The American public should not have to choose between a system that makes their PII vulnerable to scammers or one that permits intrusive government surveillance.

SARs are an essential tool for identifying suspicious activities. Rather than reduce the number of filings, policymakers should seek ways to improve their utility for law enforcement and consumer protection agencies.

While some policymakers would like to raise the thresholds for filing SARs, meaningful reform will require leaders to look beyond reducing SAR filing volume and instead consider how to make data-sharing regimes more effective. Indeed, if policy focuses on the narrow goal of reducing the number of SARs filed, then policymakers may handicap one of the best tools available to financial companies and

---

[59] 12 CFR 1005.11(c)(1).

[60] John Adams. (2024, February 1). Why aren't more banks sending real-time payments? American Banker. https://www.americanbanker.com/payments/news/why-arent-more-banks-sending-real-time-payments

[61] Jay Stanley. (2025, June 2). Digital Identity Leaders and Privacy Experts Sound the Alarm on Invasive ID Systems. American Civil Liberties Union. https://www.aclu.org/press-releases/digital-identity-leaders-and-privacy-experts-sound-the-alarm-on-invasive-id-systems

regulators to prevent fraud and scams.[62] It's the actionability of the data in the SAR, and the utility of systems to support law enforcement activities efficiently, that must be addressed.

The key question, from the perspective of providing relief to scam victims, is how to improve reporting to better highlight the activity affecting regular people. If data collected from SARs can help law enforcement agencies (LEAs) better analyze scam trends, it will improve scam detection and prevention and support ongoing investigations. This is an efficient step to put existing resources to use for additional problems.

LEAs can access SARs through the FinCEN web portal. With the portal, they can query data by using FinCEN Query or download data in bulk to run on separate systems. LE agencies must apply for access to the FinCEN portal. If FinCEN approves the request, it executes a memorandum of understanding (MOU) with the agency. Last month, the Office of the Inspector General reported that FinCEN had approximately 450 active MOUs with external agencies and 14,000 external users.[63]

The ability to obtain bulk data is critical for any user seeking to apply SARs to analytical platforms. Once uploaded, platforms can conduct data mining and other analyses to permit greater utilization of SARs. But those LEAs face hurdles because uploading is time-intensive. Many key data points are buried in narratives, requiring costly machine-learning techniques to extract them. An updated SAR form could require the critical fields in a structured format, reducing burdens on both private institutions and LEAs.

SARs can become the signals that connect filings across accounts and institutions lead to new cases. But SARs themselves are not legal evidence. LEAs use SARs, in part, as tips on where to issue subpoenas. As the Chief of the IRS's Criminal Investigation unit recently wrote, "BSA data is often the first signal that something isn't right. These filings become essential puzzle pieces in identifying patterns, following financial trails, and building cases that protect taxpayers." The IRS conducted 3.9 million searches of BSA filings in 2025. That data was the basis of a new investigation in more than 2 of every 3 instances. The same report noted that SARs were used to initiate cases under 12% of the time, but SARs were queried on targets in over 80% of their cases, suggesting connected activity is a critical area done well.[64]

For this reason, it is important for policymakers to consider ways to reshape how SARs data is collected, stored, and shared.

Migrate data from unstructured "narratives" to structured formats. Some of the most useful information is filed in non-structured data fields. Filers use these sections to explain details that are not easily conveyed elsewhere in the form. To their credit, the narratives often contain valuable descriptions of activity. Often, filers put the most useful information in the narrative section. Nonetheless, for analysts seeking to identify trends from large numbers of filings, information stored in non-structured fields is

---

[62] Kelly Phillips Erb. (2026, February 27). Following The Money: How Financial Data Helps Solve IRS Criminal Cases. Forbes. https://www.forbes.com/sites/kellyphillipserb/2026/02/27/following-the-money-how-financial-data-helps-solve-irs-criminal-cases/

[63] Office of the Inspector General of the Department of the Treasury. (2026). Audit of FinCEN's Management of BSA Data—User Access and System of Records Notice (OIG-26-015). https://oig.treasury.gov/system/files/2026-02/Audit-of-FinCEN%27s-Management-of-BSA-Data---User-Access-and-SORN-%28OIG-26-015%29---SECURED.pdf

[64] Internal Revenue Service. (2026, February 24). *IRS-CI data shows BSA filings are used in nearly all its investigations*. Press Release. https://www.irs.gov/compliance/criminal-investigation/irs-ci-data-shows-bsa-filings-are-used-in-nearly-all-its-investigations

hard to use. Unfortunately, this information is difficult to access because it is not in a structured, searchable format. With better structure, law enforcement can more effectively use existing data.

SARs should have a clear identifier for activity involving scams.

Policymakers should design data collection to help LEAs see scam activity. With a simple "check box" to identify a scam event, consumer protection agencies could rapidly search SARs to identify scam victims. The inclusion of the box would help LEAs and lead to better outcomes for victims. Already, systems like FedNow's FraudClassifier and ScamClassifier capture useful data on fraud and scam transactions. Relatedly, SARs should include contact information for scam victims to facilitate LEAs and consumer protection agencies' ability to help victims and potentially provide remedies.

Do not raise thresholds for currency transaction reports (CTRs).

Notably, the IRS reports that the median size of a CTR used in a 2025 investigation was $12,543, underscoring the importance of not raising filing thresholds.[65]

It is also the case that raising thresholds would close off the line of sight for LEAs to some categories of scams. For example, most transactions in teen sextortion cases are for only a few hundred dollars. The most common payment types in these events were, in order: gift cards 25.6%, PayPal 17.8%, Venmo 9.4%, Zelle 7.5%, Apple Pay 4.8%, and cryptocurrency at 2.9%.[66] Laws curb teens' access to traditional bank accounts, but there are still loopholes, such as gift cards, teen accounts, and accounts held by parents. Teens authorize transfers under coercion that criminals will distribute explicit images.[67] Criminals on the dark web are not seeking to raise thresholds for information sharing. Our law enforcement agencies should not raise them, either.

Clarify to banks that they can release bank account information to law enforcement agencies. For their investigations, LEAs need to know where the money was sent. It is essential to include the routing and account numbers for destination (funnel) accounts. This privilege does not infringe the privacy rights of victims who sent funds, unlike if an FI released this data to a private individual. With this information, LEAs will have more resources to track patterns. Again, it is important to identify the vulnerabilities in the payment ecosystem, starting with the "bank of the criminal." Anecdotally, some banks appear to believe they cannot release this information. Regulatory clarity is needed. Otherwise, LE needs to issue a subpoena to the SAR filer, wasting precious time.

Conclusion

Financial fraud and scams are among the most serious and rapidly evolving threats to American consumers. The stakes could not be higher. Reported losses now exceed $12.5 billion annually, and the true toll is far greater. Seniors are losing their life savings. Service members stationed overseas cannot access frozen funds. Teenagers are being extorted. And the criminal organizations behind these schemes

---

[65] Ibid

[66] Jimenez, A. (2024, November 21). Teen Sextortion Victim Payments. Dynamic Securities Analytics, Inc. https://securitiesanalytics.com/teen-sextortion-victim-payments/

[67] ibid

are growing more sophisticated, better resourced, and increasingly intertwined with broader networks of transnational illicit finance.

The good news is that the tools to fight back exist. Supervision works. Enforcement works. Shared liability works. The evidence from Zelle's belated safety improvements, from the reduction in overdraft fee harvesting, and from the United Kingdom's successful implementation of the Contingent Reimbursement Model all point to the same conclusion: when regulators hold institutions accountable, the financial system becomes safer for everyone.

But sadly, in the last year, policy has had the opposite effect. By sidelining the CFPB and preventing it from supervising payment apps and digital wallets, the Administration and Congress have reduced our defenses against scams.

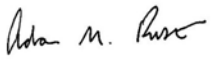
The Consumer Federation of America urges Congress to take the following actions:

- Restore the CFPB's funding to the 12 percent cap established in the Dodd-Frank Act and reverse the dismantling of the agency's supervision and enforcement capacity.
- Reestablish the CFPB's authority to supervise non-bank payment apps and digital wallets, including products that facilitate digital asset transfers.
- Pass the Protecting Consumers from Payment Scams Act to extend EFTA protections to consumers induced through deception or coercion, share liability between sending and receiving financial institutions, and expand coverage to wire transfers.
- Support regulation of crypto kiosks, including transaction limits, mandatory holds, fee caps, and scam warnings.
- Pass the Safeguarding Consumers from Advertising Misconduct Act to hold social media platforms and telcos accountable for their roles in facilitating fraud and scams.
- Improve the structure and utility of SARs so that law enforcement and consumer protection agencies can more effectively identify scam victims, track criminal networks, and build cases.
- Resist efforts to raise CTR thresholds, which would blind regulators to the low-dollar transactions that characterize many of the most harmful scams.
- Advance legislation to hold social media platforms and telecommunications companies accountable for the role their networks play in facilitating scam activity.
- Update the Electronic Funds Availability Act and Regulation CC to give receiving financial institutions the flexibility to delay account crediting when they detect suspicious activity, without diminishing consumers' core rights to challenge such actions.

The costs of inaction are not abstract. Every month that passes without meaningful reform is another month in which criminal organizations operate with impunity, consumers lose money they cannot recover, and financial institutions face little incentive to invest in prevention. The legal framework governing electronic payments was designed for a world that no longer exists. Congress has both the authority and the responsibility to bring it into the present.

It is time to advance reforms that protect American consumers, strengthen the integrity of our payment systems, and ensure that those who profit from moving money bear a fair share of the responsibility for doing so safely.

Sincerely,



Adam Rust
Director of Financial Services
Consumer Federation of America
arust@consumerfed.org

Chairman BARR. The gentleman's time has expired.

We will now turn to member questions. I recognize myself for 5 minutes for questioning, and I will start with Mrs. Dempsey.

The recommendation of the STOP Fraud Act or updates to Reg CC to allow for exceptions in terms of holds, allowing more holds for scrutinizing wire transfers or suspicious checks. We hear a lot about—especially from community banks—concerns about rewards in payment stablecoins. This seems to kind of go in the opposite direction but I think banks will always—and credit unions, frankly—all community financial institutions will always be here, even with the advent of blockchain technology and stablecoins, because of the fraud prevention that you all and the trust that you all create and why you are even more important in the ecosystem with the advent of stablecoins.

Can you talk about that? Does this—I think it is a good idea to give you more flexibility on holds, but does that work at cross-purposes in terms of the concern about disintermediation?

Mrs. DEMPSEY. It is a broad question.

On the Reg CC side for holds, yes, definitely giving more leeway there for the banks.

The language right now is a little vague on if you have a reasonable cause to place a hold for longer, a longer period of time. So a lot of banks are not apt to use that to extend their hold times when they see those fraudulent checks when they come in.

With checks 21 years ago, everybody thought checks were just going to clear instantly and that you would be able to catch those fraudulent checks that were presented into the system, but we still see that it can take several days sometimes for a check to clear.

Also, it takes a lot of time, especially when you are talking about altered checks that have occurred in the mail, for the small businesses, that they may have been stolen out of the mail and then come out of their account.

I would love for them to check those accounts every single day and to make sure that the payee matches who they sent it to, but, unfortunately, they just do not.

Even with the education that we provide to those small businesses—we host small business luncheons to train on fraud and scams and to show them what to look for—but when you extend that hold time, it gives that customer even more time to check their online banking, to look at those accounts, and then for us to return those. Because that is one of the hardest things, is the midnight return that we have with checks and dealing with trying to mitigate those and to solve those.

Chairman BARR. Well, just to sum up, we are embracing the innovation and moving toward a more frictionless payment system, obviously, with the GENIUS Act, but banks and credit unions will always be needed, I think, to build in wanted and needed friction to prevent fraud.

Mr. Schuster, I have heard from financial institutions that when they implement robust fraud controls, they can face allegations of unfairness or abusiveness under CFPB's UDAAP authorities, especially when interventions might create necessary friction for customers.

My Rectifying UDAAP Act requires the CFPB to provide clear standards for what constitutes a UDAAP violation, giving financial institutions the clarity they need to serve customers, including protecting them from fraud and scams.

From a legal perspective, how does UDAAP risk currently influence institutions' willingness to deploy proactive risk-based fraud controls and do you think that greater clarity in the form of my bill, the Rectifying UDAAP Act, would reduce hesitation around reasonable, good-faith fraud interventions?

Mr. SCHUSTER. Thank you. It is a great question. Yes, your act would certainly help financial institutions.

They right now face the decision of am I going to address this fraud or scam as it currently exists under existing statutory law but risk being criticized from an unfairness or an abusive perspective from their regulators and supervisors, and they will many times look at the potential financial impact to them of a compliance rating versus providing money to an individual who has been taken advantage of by a scam.

When they are implementing tools, it is the same thing, that regulators are not looking at how artificial intelligence works, advanced technologies work. They have an aversion to doing that, and there is a belief that is unfair, that is abusive. They need to look at that, and your bill would certainly help.

Chairman BARR. Ms. McKune, your testimony was that Park Community Credit Union prevented more than a million in fraud losses for your members. That is fantastic.

Can you describe in more detail what those fraud attempts look like on a day-to-day basis and the staff time, compliance oversight, and technology investment that is required to manage all of this?

Ms. MCKUNE. Thank you, Chairman.

We work every day to run investigations quickly. We have full-time fraud staff. We have deployed technology to catch and alert and indicate to us where there might be suspicious activity.

We have, obviously, a compliance team that works hand in hand with the fraud team to ensure that we are meeting our compliance and regulatory obligations in that regard.

There is a sign in our fraud department that says: How many days since the last fraud incident? It never leaves zero because what we do every day is keep vigil and work to investigate to see whether we are having an individual problem, whether we are seeing multiple members affected by a scam. So we are very conscientious about balancing their needs with the burden on our side to ensure we are protecting them.

Chairman BARR. Thank you. I know it is a very costly enterprise.

My time has expired. Dr. Foster is recognized for 5 minutes.

Mr. FOSTER. Thank you, Mr. Chair.

Mr. McDade or Mr. Rust, as I mentioned in my testimony, identity fraud and impersonations are crucial to every one of these scams and they are becoming a greater threat to American consumers, particularly with the proliferation of artificial intelligence and deepfakes.

Not only are the scammers able to reach more potential victims by automating these, but their scams are much more sophisticated. The old schemes of having typo-ridden emails claiming you are the

beneficiary from a distant relative have sort of been replaced by very sophisticated impersonations, which can be online videos, things like that.

It is only going to get worse. The rise of agentic AI is going to generate a huge new wave of these frauds where, when my agent starts talking to your agent to do a business deal or to just communicate, the very first question is going to be: How do I know you are who you say you are and not some scammer?

So I think that having a secure digital identity for Americans that want to be able to prove they are who they say they are is going to be a crucial tool.

I worry that America is falling behind the rest of the world in this because, by the end of this year, every citizen of the EU, if they wish, will have a tool to get out their cell phone, smile at it, do the biometric log-in, present an identity app that proves they are who they say they are.

In the absence of any action by the Federal Government, States are rolling out digital driver's licenses. Sort of ironically, it is the National Institute of Standards and Technology—the U.S. standards—that are being deployed all around the world. They are on every iPhone and every Android, but we are not using them federally to prevent identity scams. So I think that is a real missed opportunity that we would like to.

Also, Mrs. Dempsey, you highlighted bitcoin ATMs. I would urge every member of this committee to just go look at their hometown, do it on Google Maps, and then go do a search for bitcoin ATMs. Then maybe do a search for where all the nearby fentanyl deaths have been and see if the maps look kind of similar. These are tools by drug dealers, they are tools by scammers, and we have to do something about that.

During the previous Trump Administration, actually, Secretary Mnuchin had the simple suggestion that why do not we have mandatory Know Your Customer (KYC) on all crypto wallets, which I think would solve a big part of this problem anyway.

So any thoughts you have on that, Mrs. Dempsey? What should we do about the bitcoin ATMs? Because they are not a small problem.

Mrs. DEMPSEY. Yes. The bitcoin ATMs, in my opinion, are just nefarious, and there is nothing good in our community taking place at a bitcoin ATM. There is no need for them.

To your point, once they enter that, they are gone. There is no tracking. From where we stand, there is no getting that back.

So I know there are several States that have enacted laws. Our State is currently entertaining some laws dealing with bitcoin ATMs and placing limits on them and placing warnings on them to help educate the consumers and to protect them.

Mr. FOSTER. Yes, but that is not going to help someone who has been scammed, a romance scam. I know, I am familiar with a bar owner who was given a couple hundred bucks a week to put a bitcoin ATM in their bar, and after a couple weeks he said, "Get this the heck out of my bar" because he was sick and tired of seeing elderly people pouring their life savings down the bitcoin ATM crying as they did it.

Mrs. DEMPSEY. Yes. If there were regulations, even if they did put it in the ATM, where they had a certain amount of time to get it back, even things of that nature could help protect them when they fall victim to those scams.

Mr. FOSTER. Mr. Rust, how would you generally rate the position of U.S. citizens in terms of being able to prove they are who they say they are, to know that the person they are talking to is a real person in an online environment? How does that——

Mr. RUST. So this problem is not working now and getting worse. You can imagine with deepfakes and voice cloning that fraudsters are going to gain new advantages to harm people. That seems inevitable.

Probably the best—Michael Hsu made the point that the best way to fight AI fraud is with AI technology, supervisory tech but we need to invest in that. We need to be able to buy those from regulators to have the tools that the fraudsters have.

Mr. FOSTER. Does anyone know—have comments on where AI—the thing that interests me are these personal AI assistants that everyone is going to use, which could be the last and best line of defense. So when you get that first phishing scam mail, you have your personal AI assistant say "warning," warn you so that your elderly parents will never even receive that scam communication.

Are there efforts ongoing to make personal assistants that will filter that stuff properly, or is that another missed opportunity?

Mr. RUST. I mean, this is about having bots to stop bots, and with more platform involvement it will be more urgent.

Mr. FOSTER. Thank you. Yield back.

Mr. MEUSER [presiding]. The gentleman yields back.

The gentleman from Arkansas, the chairman of the full Financial Services Committee, Chairman Hill, is now recognized for 5 minutes.

Chairman HILL. Thank you, Mr. Meuser. Appreciate that.

Let me start with you, Mr. Schuster.

This has been a good discussion so far, but I wanted to get into this idea of collaborating to fight fraud.

Under the Fair Credit Reporting Act, entities that aggregate consumer information and provide outputs used to make eligibility determinants are often deemed consumer reporting agencies, which carries a lot of compliance regulations and compliance burden, which is probably right, including responsibility for accuracy and dispute resolution and things of that nature but we also are seeing a lot of financial institutions explore this kind of consortium-based fraud fighting.

When I was a banker, we had a phone call every Wednesday in my hometown, and it was an off-the-record phone call that probably does not comply with Federal law or regulation, but it was essentially the ops people in every bank in town saying, "Have you seen somebody wander into the lobby that is doing this?"

It is an early warning system, and it is, like, classic American protecting the community, working with each other in a consortium basis but were we to do that in an analytic way using some sort of a more formal system, do you see that people are afraid to do that because of falling under the—that shared information falls

under that consumer reporting agency designation? What could we do about that?

Mr. SCHUSTER. It is a great question.

Fraud identification is inherently pattern recognition. The more information and data that you have, the easier it is to identify patterns that are abnormal, where there is fraudulent activity happening.

Currently, the Fair Credit Reporting Act has very broad definitions, and financial institutions, their service providers, technology providers are hesitant to share data that they have that could be used for that pattern recognition, the fraud identification, earlier.

If there were clarity or a safe harbor under the Fair Credit Reporting Act about sharing data for fraud or how that data could be shared, it would vastly improve financial institutions' and all these other companies' ability to share that data and have it available to prevent fraud.

Chairman HILL. Thank you. That is helpful. If you have got specific ideas of how one might craft a safe harbor like that, I hope you will share those with the committee.

Ms. McKune, let me turn to you from an institution point of view.

We know that scamming, as we have all heard today, has become more sophisticated, using AI and deepfakes and forged documents, and we have got people wandering in courthouses and wandering in bitcoin ATMs and wandering into banks. We know all that, and we are all trying to come up with the best whole-of-government approach to fighting that, but a lot of it falls right back to those financial institutions.

Are you trying to use these promising technologies to fight against the scammers that are using technology and do you have comfort with that? Do you have a lack of training? Do you have a lack of talent in your institutions? Tell me a little bit about that.

Ms. MCKUNE. Thank you for your question, Mr. Chairman.

We certainly are trying to use technology prudently, cautiously, thoughtfully. We want to make sure that we are at least trying to keep pace with the fraudsters.

There is always a question in small financial institutions of the cost and of the adoption and of the relative sophistication of both our members and the fraud community in which we sit but we do want to be able to respond faster and all of those tools—the all-of-government approach, the regulatory reforms, possibly safe harbors—would play into our layered approach.

Technology is a piece of it, but one of the things that we try to pride ourselves on as credit unions is our ongoing member-to-member—our relationship with our members and our ability to see them and see what is an aberrant transaction, and try to use our judgment.

Chairman HILL. On a share draft—passing a check that has been washed, for example—are you seeing good cooperation for filing a police report in your area? Are you seeing postal inspectors being helpful or local Secret Service? Tell me about that.

Ms. MCKUNE. We are always grateful for the law enforcement engagement that we have. We often run up against law enforce-

ment's limitations in terms of resources and their ability to drill in on the harm that we are seeing.

One of the things I think is really important to note is that the number of resources that law enforcement can invest often is tied to the amount of the loss, and the amount of the loss could be absolutely ruinous and devastating for our individual members and not be of a size or of a frequency that law enforcement can really lean in.

Chairman HILL. Thank you very much.

I yield back, Mr. Chairman.

Mr. MEUSER. The gentleman yields back.

The gentlewoman from California, the ranking member of the full committee, Ms. Waters, is now recognized for 5 minutes.

Ms. WATERS. Thank you very much. Absolutely delighted to be here at this hearing. I am so surprised that the opposite side of the aisle have decided to talk about fraud and abuse.

Since Trump and his return to the White House, Trump and his family have made billions thanks to their growing meme coin schemes. At the same time, families are more vulnerable than ever to financial abuse as Trump pushes a reckless deregulatory agenda.

He has dismantled the CFPB—that is the Consumer Financial Protection Bureau—rolled back consumer protections, and dropped lawsuits against big banks and crypto scammers, making it easier to cheat everyone—from retirees, students, and working families—while he and his family cash in.

Mr. Barr's bill would weaken UDAAP—that is U-D-A-A-P—authority to the detriment of consumers. Of course, we need stronger protections, not less and I just want to raise a question about all of this that we see coming at the very top of government.

Mr. Rust, we have been getting mixed messages from President Trump where, on one hand, he claims to care about the affordability crisis and says Congress should enact a law to cap excessive credit card interest rates at 10 percent, but on the other hand, he says it is a hoax and has worked with congressional Republicans to slash the budget of the Consumer Financial Protection Bureau, the Federal watchdog for consumers in the financial marketplace. They have also blocked rules like curbing excessive credit card fees.

So, Mr. Rust, when the CFPB issued its larger participant rule to supervise Big Tech payment apps, banking groups were supportive of the effort as a way to level the playing field.

Should Congress revisit this issue and require the CFPB to immediately begin examining the large payment apps and mobile wallets provided by Big Tech? Could this help identify payment scams happening on these apps sooner?

Mr. RUST. Thank you for the question.

Yes, absolutely, Congress should restore the CFPB's authority to supervise payment apps and digital wallets. This is sort of the baseline way to address scams. Access to looking at the activity on these networks is how regulators can spot things, how law enforcement can spot things.

UDAAP is the tool we have if EFTA is not restored to protect consumers. UDAAP was the tool used for the Zelle enforcement action. Again, the CFPB needs to be back in the game.

Ms. WATERS. Well, thank you very much.

I am going to go back to the CFPB because many of us have worked so hard. In Dodd-Frank, we gave the CFPB authority to stop unfair, deceptive, and abusive acts and practices by bad actors.

So if the Congress of the United States wanted to do something about fraud, unfair, deceptive, and abusive acts, why do not we just make sure that the CFPB can do what we organized it to do rather than being attacked constantly by the opposite side of the aisle and the President of the United States of America? Would it not be just simple to allow them to do what we organized them to do?

Mr. RUST. We should immediately restore full funding for the CFPB.

Ms. WATERS. Are you aware of the CFPB and how much money they have returned to consumers?

Mr. RUST. The CFPB has returned over $19 billion to consumers. That is a direct way to benefit consumers. I cannot think of something that makes a greater difference than when you have been harmed and an agency is responsive the way that CFPB is.

Ms. WATERS. I consider this one of the most dangerous things that have been done by the President of the United States of America, with a clear message to consumers to say that he cares about the big boys who are ripping off and who are creating this fraud and does not care about the consumers whom we, on this side of the aisle, have tried to protect. We have worked very, very hard.

I am so pleased that you are here today, that everybody is here today. Let the truth come out. Let the truth come out and people know where the fraud is really coming from and that the opposite side of the aisle is not doing a darn thing about it.

Chairman BARR [presiding]. Well, reforming UDAAP would be helpful.

The gentleman from Texas, Mr. Williams, is now recognized.

Mr. WILLIAMS of Texas. Thank you, Mr. Chairman.

I thank all of you for being here today.

I am a small business owner in Texas, and for 57 years community banks and credit unions have kept me going every single day.

Many scams targeting small businesses involve criminals impersonating vendors, bankers, or contractors, and these scams often start through spoofed phone calls, email promises, and PR social media messaging before the transaction even reaches the banking system.

Once the payment is sent through wires or peer-to-peer transfers, it can be extremely difficult, as we have heard already, to recover these funds.

So, Mr. McDade, how frequently are banks seeing this type of fraud against their small business clients, like myself, and what warning signs would small businesses look out for?

Mr. MCDADE. Thank you for the question.

Banks are, unfortunately, seeing this very often, and it is only increasing.

Recently, we have seen very specific impersonation scams that are related, unfortunately, to the Paycheck Protection Program (PPP) loans that were taken out to help small businesses during COVID.

A lot of that information is posted publicly in many places, and so the scammers are able to go out on the web and locate where these small businesses bank through their PPP loans.

They can even go so far as to get who the individuals are, in many cases, working at these small businesses, their information. They can then call the banks representing that they are that person and learn who their relationship manager is.

They will then spoof the banks' phone numbers and try to contact these small businesspeople to perpetrate fraud. They will get a text message saying: Did you send this wire to another company? Yes or no? They will respond no, and they will immediately get a call from somebody representing that they are the very bank that they bank with.

Unfortunately, they are talking to a scammer and this scammer then will tell them: To make sure you are who you say you are, please read back the code that I am sending you. That code will be, unfortunately, a one-time pass code as the scammer is trying to access the person's account online and do an account takeover.

This sort of activity is becoming rampant, and these impersonation scams are especially dangerous because they are also eroding the trust between the financial institutions and our own customers.

What banks are doing in response is we are educating our customers. Our specific bank reached out to all of our PPP customers and let them know about this scam. We encouraged them, if you ever get a call or a text from our bank that does not seem correct, call your relationship manager back directly and talk to that person.

I can tell you, from my experience on the CBA's Fraud Management Committee, it is not just our bank. It is all the banks on the committee who have small business relationships are seeing this exactly same thing, and the collaboration that the CBA brings between us is really helpful.

Mr. WILLIAMS of Texas. Okay. Thank you.

Community banks play an important role in protecting your customers from fraud, but they are also dealing with a growing wave of check fraud, including checks stolen from the mail, altered checks, and counterfeit cashier's checks.

When fraud occurs, smaller institutions often have to spend significant time and resources investigating claims, navigating liability disputes between financial institutions, and attempting to recover funds, and that puts people like me on the back burner to get a loan that we may need.

So, Mrs. Dempsey, when a community bank spends time and resources dealing with check fraud disputes, what does that mean for their ability to focus on serving customers, like our small businesspeople across this country, and lending in their communities?

Mrs. DEMPSEY. Thank you for the question.

You are correct. Check fraud, especially in a small bank like mine, takes a tremendous amount of time and the majority of the check, as Ms. McKune referred to, so many times the checks are of an amount that it is not going to engage law enforcement, and it is also not going to warrant us fighting legal battles to try and

get that money back. So it is taking all that time to work through that process.

I will say, for our bank, if you had a check stolen out of the mail, we give you money or give you credit back immediately to your account when you identify that. So we work really closely with our customers to not put them in a position of not having access to those funds but you are correct; it takes a tremendous amount of my time, from the CEO down to all of our operations department to our front line, in dealing with that daily and then working with those customers to do that, and that is time that we could use working with our small business owners, showing them new AI, new things that they can use, new payment systems that they can use to help them be more efficient and to grow their businesses.

Mr. WILLIAMS of Texas. Thank you.

Ms. McKune, I have a short time to go here, but in your testimony you highlighted the importance of consumer education.

What types of outreach have credit unions found most effective in helping members recognize fraud attempts?

Ms. MCKUNE. Thank you, Congressman.

We have tried to use multiple approaches to ensure that different messages are getting through and that the most important messages do not get lost in a lot of communications. So we often will put information in our social media, we will put information about active scams as banners on our website, as landing pages on our online banking but we also do a lot of work. We are a community development financial institution, and we do a tremendous amount of work in our communities to try to ensure that folks understand what risks are out there and how their accounts really work.

Mr. WILLIAMS of Texas. Thank you. My time has expired.

Chairman BARR. The gentleman yields.

The gentleman from Georgia, Mr. Scott, is now recognized for 5 minutes.

Mr. SCOTT. Yes. Thank you, Chairman.

Mr. Rust, let us get to the heart of the matter.

In your opinion, what is the level of damage this is doing to our overall economy?

You mention a lot of this rests in what you refer to as this critical gap. What do you mean by that? What is the level of economic damage that our failure to address this critical gap that you talk about?

Mr. RUST. Thank you for the question.

Mr. SCOTT. What is the damage? Go ahead.

Mr. RUST. We see reports of $16 billion in fraud losses, but research suggests that is possibly even 20 times less than the actual number because people feel shame, people do not know where to go, so they do not report it. The impact on their household is destabilizing, possibly crushing, so that affects our economy.

The critical gap? I see a critical gap between the work that is occurring to stop some of these overseas criminal organizations that are already working to move money, money laundering, human trafficking, they are also doing scams. That is their new line of business, and we should be eliminating silos between consumer protection agencies and those agencies, and possibly we should also be thinking about when there are enforcement penalties for BSA/

AML violations, that if there are scam victims involved, that should be a way that they receive a remedy.

Mr. SCOTT. What do you feel we here in Congress can do about this? I mean, are we doing enough? Do we address this critical gap through legislation or is this a money problem of us not punishing these persons who are doing this wrongness?

Mr. RUST. So, yes, sir, I believe this is a bipartisan solution. I believe there is bipartisan interest to fix this.

Congress can do a number of things. They should refund the CFPB to begin with. They should restore the payment app rule, that would make a big difference. I think they should look at many of the solutions you have heard about, information sharing and giving more line of sight between institutions.

Because all of this involves networks. This never is just the send side. It is always receive side as well. So we can make changes. Congress can do a lot.

Mr. SCOTT. Yes. So you feel there is nothing more that we need to do as far as dealing with the Bank Secrecy Act itself? Are there things we need to do to make it stronger, or do you feel that the act is doing enough?

Mr. RUST. Well, there is plenty that could be done on that side because that is where law enforcement, where those organizations are sharing information, receiving SARs, assessing problems, and highlighting it for other organizations.

So, for example, the conversation about SARs is really central here, and providing ways for that information to highlight scams I think is critical.

Mr. SCOTT. Well, thank you very much.

I think we need to really focus on what we can do about this, because if we cannot deal with this, the critical gaps that you are talking about here, there are things we have got to do here in Congress to address this.

So I appreciate your comments. Thank you.

Mr. RUST. Thank you, sir.

Chairman BARR. The gentleman yields.

The gentleman from Michigan, the vice chair of the committee, Mr. Huizenga, is now recognized.

Mr. HUIZENGA. Thank you, Chairman Barr.

With readily available information and images that are out in the general public on the internet and other places, there are many, many people who are victims as both scam targets and as vehicles to go after those victims.

A couple of years ago our office heard from someone whose mother was in an online relationship with an individual. I will call that individual Individual A. While using AI, the scammers put Individual A's face on a decorated military officer's body, put that face on someone who was being cared for in a hospital, and it is amazing, really, truly unbelievable how authentic the images looked, because I was Individual A.

To be clear, there was no online relationship. It was someone who had taken my readily available information and my images and had used AI. I think it just demonstrates that, frankly, no one is above being caught up in those scams that are going on right now.

Sadly, the individual's mother had sent thousands of dollars to someone in Vietnam. We worked with Facebook where the images had appeared to have them removed, but they kept reappearing.

Mr. Schuster, I am curious, how much fraud originates actually outside the banking system entirely, such as with social media, telecom networks, or overseas criminal operations?

Mr. SCHUSTER. It is a great question. I think the majority of it.

Financial institutions at the end of the day are just where the funds ultimately derive for the scams, for the fraud, that originates elsewhere.

What used to be in a physical place that somebody was obtaining money is now all digital. Payments are faster than they have ever been.

Those technologies that you are talking about are what are used to start fraud, and financial institutions need the abilities to do that pattern recognition. They need clear guidance.

Their regulators need to permit them to use these technologies from a UDAAP perspective and other things, so that if there is something that is happening that happened upstream from the financial institution—which is where it originates—they can address it.

Mr. HUIZENGA. If most scams originate outside of financial institutions and payment networks, is it fair to place the majority of regulatory burden on those banks and payment providers?

Mr. SCHUSTER. I think it would be great if we gave those financial institutions and payment providers more tools even before we think about liability.

I think that we are thinking about liability after a fraud or a scam has occurred. If there is something that they can do to help people prevent these types of things, that would be great.

I also think that looking at some of those other areas that you have been discussing, social media and elsewhere, that is where there should be focus, too.

Mr. HUIZENGA. I do want to hear from our bankers, as well. Very quickly, how do you think we can improve consumer education and outreach on fraud and scams?

Mr. SCHUSTER. I think that it is something that if financial institutions are given the tools, or less restraints with respect to how they can look at these items and what they can do to communicate with their customers from data that they have from other institutions, from their service providers, from financial institutions, they will be able to share more specific information and education with consumers that will be extremely helpful.

Mr. HUIZENGA. How about Mrs. Dempsey and Ms. McKune?

By the way, Ms. McKune, I am going to take point of personal pride here. My future daughter-in-law happens to be from Danville, Kentucky.

For those of you not aware, Danville is quite a small town, as I understand. So I am looking forward to having her in the family soon, but what is your experience with your customers?

Ms. MCKUNE. One of the things that we think is really key is the ability to share information more broadly. When we are constrained, even in just dealing with our respective counterparts in the banking realm and financial institutions, the information we

can share is limited and the information that would be helpful is often out of our reach.

We are talking about a very time-sensitive exercise, and we are talking about something that happens really quickly, and with regulatory constraints on how long we can find a pause, that is difficult.

I think it is worth exploring information sharing that goes beyond thinking about financial institutions because so much fraud originates in spaces for which we do not have a vantage point.

Mr. HUIZENGA. Mrs. Dempsey, 10 seconds.

Mrs. DEMPSEY. I would just concur. More information sharing is critical between banks.

We have had experiences with banks where we call and they will not give us any information just because of fear of the sharing information, even though it should fall under the current regs now that they are able to share with us and they do not and then just she mentioned consumer education. We are constantly educating, whether it is through in-person, whether it is through luncheons, online, face-to-face. I have been on the radio. We have weekly articles in our local newspapers.

So we are doing everything that we can to make consumers aware of the frauds and scams that are out there, but they change every day.

Mr. HUIZENGA. Thank you. I yield back.

Chairman BARR. The gentleman from California, Mr. Sherman, is now recognized.

Mr. SHERMAN. Consumers face two kinds of rip-offs: those from big institutions that do provide a useful service but sometimes engage in misleading and confusing practices.

The chief defense here was the CFPB, which provided almost $20 billion in returned money, $5 billion in civil penalties, $363 million back to veterans and that is just the retribution part. Think of the deterrence. Think of all the scams that never happened. Think of all the corporations that said, "We will never get away with that."

So we should not defund those who police our streets. We cannot defund those who police the suites, the corporate suites but today's hearing tends to focus on the full-time criminals who provide no useful services at all, just rip people off.

Mr. Rust, thank you, first, for the work of the Consumer Federation of America over the many decades. You have talked about the Suspicious Activity Reports that financial institutions file and the need to allow law enforcement to see patterns, to look not at just one item, but what is happening across the country.

We could provide that the Suspicious Activity Report includes at least two identifiers, both a driver's license number and a Social Security number or a passport number.

We could reduce the importance of the narrative portion of the report that cannot be correlated with other reports and go more to structured fields.

What can we do to make sure that a Suspicious Activity Report does not just tell you about one instance, but allows you to link it with what is happening elsewhere?

Mr. RUST. So this is about appending data and being able to see patterns. Structured information is great for searching. If you are

familiar with the Home Mortgage Disclosure Act, that database, everything in it is searchable. It is all structured.

If you are a local law enforcement agency working in a State, the ability to search for where that scam occurred is very valuable.

The ability to see where funds have transferred across financial institutions, you need to be able to track account numbers, device IDs, things like that. Those are tools that law enforcement needs to build cases against these kinds of situations.

So SARs are a tool where the underlying facts can lead to subpoenas that can lead to stopping the problems.

Mr. SHERMAN. Thank you.

I want to commend our ranking member for his idea that we need Know Your Customer to apply to all of the wallets, crypto wallets.

One issue comes up where an entity impersonates a financial institution. Reuters claimed that Meta had 10 percent of its revenue, roughly $16 billion, derive from advertisements for scams and banned goods.

Credit unions came to my office and identified a system where a scammer pretends to be your credit union or your bank, so you trust them, and all of a sudden you are wiring $500, you are giving out information. A lot of this comes from advertisements where Meta will let you pretend to be a financial institution when you are really not.

Mr. McDade, what can be done to make sure that Meta and similar organizations are not running ads in the name of a financial institution when it is really a criminal?

Mr. MCDADE. Well, I would first point to the SCAM Act sponsored by Representative Meuser. The reality is we are absolutely correct that one of the largest threats that we have is banks, the misinformation that happens outside of our control environment. Most of the scams——

Mr. SHERMAN. And you live with Know Your Customer and Meta does not know anything about its advertiser.

Mr. MCDADE. Well, that is correct. The study that you cited specifically notes that it is a situation where Meta is putting forth knowingly fraud information into the ecosystem.

Mr. SHERMAN. Got you.

I want to get one other thing, and that is we need payee matching so that when you wire money to account number 12345, because it is supposed to go to Santa Barbara escrow, that is an account of Santa Barbara escrow.

Because we have seen again and again people lose their down payments, somebody is impersonating the escrow company, the title company, and all they have to do is scam you into their numbered account.

Britain has payee matching. We need it, too. Several chairs of the Fed have said they would work on it and still have not.

Chairman BARR. The gentleman's time has expired.

The gentleman from Georgia, Mr. Loudermilk, the vice chair of the subcommittee, is now recognized.

Mr. LOUDERMILK. Thank you, Mr. Chair.

Before my remarks, I would like to submit this letter from the American Securities Association into the record. The letter stresses

the importance of closer collaboration between financial institutions and law enforcement to combat fraud and scams. I would like to submit that for the record.

Chairman BARR. Without objection.

[The information referred to can be found in the appendix on page 147.]

Mr. LOUDERMILK. Thank you, Mr. Chairman.

I would be amiss if I did not bring up something that this committee has already done to help reduce fraud by removing the noise of nonapplicable data when it comes to looking for suspicious activities, and that was my Financial Thresholds Modernization Act, which modernizes the CTR and SAR process to reduce the burden on financial institutions so you can focus on what is actually suspicious activity versus what you identify as normal activity, and it reduces the proverbial haystack within the government so we can actually find the needle.

So I encourage my colleagues on the other side to get on board and help us move through the House this important piece of legislation that I think will go a long way to help identify fraud.

I have heard a lot about data sharing here today, and that is extremely important when it comes to collaboration between financial institutions and law enforcement and other entities, especially when we live in a day and age that the amount of data is unprecedented that is available and out there.

When I worked in IT and security and in intelligence, it was not the thought of if the data was going to be hacked or disclosed, it was when. The idea is to just make sure that your data is more secure than the other data so they will go after the other person and so I think we have to be extremely vigilant.

Mr. McDade, how can we strike the right balance between promoting necessary data sharing and avoiding excessive centralization of sensitive information, which could actually amplify the amount of sensitive data compromised in a breach?

Mr. MCDADE. Thank you for the question.

First, I would echo some of my colleagues saying a safe harbor for banks to share this essential information.

When banks are interacting in the fraud space, we are on the same team, and our fraud fighters are all working together to try and stop a fraud or scam from happening.

If we are prevented due to the amalgam of privacy laws that are being promulgated at the State level instead of the Federal level, it really creates a difficult situation for us to be able to communicate with each other.

Additionally, one of the recommendations I made in my brief was to—and I believe Mr. Rust spoke to this as well—revise the SAR policy so we have a fraud signal report and this would not be something that is a lagging indicator, but as soon as we are aware a fraud happened, have a concise way to get the metadata associated with that fraud reported to law enforcement.

If all the banks did that in the same fashion, they could immediately cross-reference that essential data and see the patterns and actually reach out and warn other banks that they might have fraudulent accounts, or even go upstream to the telecoms and so-

cial media accounts and let them know: We are seeing fraud on this phone number, or on this account, please take it down.

Mr. LOUDERMILK. Well, thank you.

One thing that I learned throughout my time in information technology and security is you do not have to protect data that you do not have and so only collect and hold that which you actually need, which, again, goes back to the modernization of CTRs and SARs.

What role can technology, such as anonymizing or otherwise protecting sensitive data, play to help mitigate concerns over information sharing?

Mr. MCDADE. I think it is essential to be able to anonymize the data in a way that protects the consumers while still giving the key data that is what we call in the industry fraud signals.

These signals are pieces of information that if they are shared across can show a pattern of fraudulent activity and point back to the source where that fraudulent or scam activity is coming from.

So while anonymizing our consumers' data is very important, the IP address, MAC address, and some of the other data coming from a fraudster's computer attacking our resources is something that we should be able to share with law enforcement at least, if not other banks.

Mr. LOUDERMILK. All right. Thank you.

I do not think I have time for my other question. So, Mr. Chairman, I will deposit my remaining time and hope that maybe I will earn interest for a future hearing.

Chairman BARR. So deposited.

The gentleman from Illinois, Mr. Casten, is now recognized for 5 minutes.

Mr. CASTEN. We may have to apply a Howey test to that deposit.

Thank you, Mr. Chairman.

Thanks to all the witnesses for being here.

I want to follow up on some questions that Dr. Foster raised at the start about bitcoin ATMs.

The FBI has reported that Americans lost a third of a billion dollars in crypt scams—crypto ATM scams—in 2025. That was a 33 percent increase from the year before. The scams, as I think many of us know, particularly target seniors.

I actually—this became personal—I got a call from a constituent earlier this month whose brother had lost $190,000, essentially all of their wealth, to one of these pig butchering scams.

I do not know the details of theirs, but for people who are watching, it is more or less as you described, Mr. Schuster. It starts on a social media, maybe it is a dating app, maybe it is your Facebook page. "I want to be friends. I am really attractive. You should talk to me. I have an investment plan."

You build these relationships and then pretty soon you need a little help to get out of a jam, or you have got an investment opportunity. "Please go to the local crypto ATM and transfer me some money now that you trust me."

It has really, I think, taken advantage of the fact that social media is almost perfectly designed to make people believe impossible things, and crypto ATMs are almost perfectly designed to monetize that lie, because once you put it in there, the transaction

is immediate, it is irreversible, it can use the ecology of the crypto system through mixers, through chain hopping, through anonymous wallets to make it untraceable.

The stories are painful. I do not know, Mrs. Dempsey and Ms. McKune, I will let the two of you argue it out who wants to take this. I am curious how your members are dealing with this, because presumably they have to come to one of your banks to withdraw real money in the first instance.

Any of you want to comment?

Mrs. DEMPSEY. Yes. Thank you for the question.

As I mentioned in my written testimony and today, it is rampant. We deal with it on the front lines. Like I mentioned, we have had multiple experiences where we have sat down with a customer and we pulled up, we literally pulled up Facebook and showed them the photo and they have told us, "Oh, they told us you were going to do that."

We have shown them FBI reports. We do everything that we can from our end when we identify those to stop it and to inform them.

As I mentioned, they are changing every week. I know every one of us could tell story after story of whether it is a pig butchering, an investment, whether it is romance, whether it is your child, your grandchild is in jail. All the things. We see it every single day.

Mr. CASTEN. I do not want this to sound the wrong way; I am sure you do that for good and ethical reasons. You also would do that because you are bound by Know Your Customer rules, right? So if they are going to withdraw the money, you need to know something about who is the identity, what is the—all the registration and reporting requirements.

Would you be supportive of rules that said let us apply those same rules to crypto ATMs, make them go through the same KYC rules so this is not all on you and your local bankers?

Mrs. DEMPSEY. Personally, yes, I think everyone should have to know their customers because I think if you know your customers, there is a lot of fraud that could be stopped at the point of origination.

Mr. CASTEN. Okay.

I want to just point out that the Trump Administration has made some positive noises about this, but everything that they have done so far has been voluntary, and I think it is pretty clear that the voluntary standards are not working.

We are seeing evidence that if one State has good rules and the other State has bad rules, the scammers will say," Hey, do not do this in Illinois, but drive across to Hammond, Indiana, and maybe use the crypto ATM over there."

So I would agree we need some policies, some Federal policies.

Mr. McDade, if you will forgive me, I was looking on your website before we got here and I saw that at EverBank you do not allow people to do ATM withdrawals of more than $2,000 a day; I think a bit more if it is a PIN-based transaction.

Is there any reason we should not employ those same standards for crypto ATMs?

Mr. MCDADE. Every institution has their own risk tolerances and sets those risk tolerances appropriately for their institution.

In my view, it would be similar to what was just said as far as the crypto ATMs. The difficulty is us being able to inform our customers that they are sending money to the right place and the right account, and the KYC rules assist with that, so on the other end we can see that this is going to a legitimate place.

Mr. CASTEN. Well, I will just close with one last story, and I would welcome any of your input. We are trying to work on some legislative fixes, and if you have good ideas, please share them.

One of the smaller towns that I represent does not have a super strong local economy. The mayor struggles to come up with enough money to pave the roads and most of their tax revenue comes from a very small set of convenience stores.

One of the convenience store owners, his primary source of—his biggest source of revenue was a bitcoin ATM, and he took it out in spite of its importance to that community because he just kept watching seniors come in every day and make deposits and then come back later and ask how to get it out.

I do not know how the people who do that look at their kids at the end of the day and say, "You can be proud of what Dad did today" but as our former colleague, Elijah Cummings, was fond of saying, "We are better than this."

Thank you. Yield back.

Chairman BARR. The gentleman from Pennsylvania, Chairman Meuser, who has done a lot of great work on this issue, is now recognized for 5 minutes.

Mr. MEUSER. Thank you, Chairman, very much.

Thank you, certainly, to our witnesses.

The FTC reported $12.5 billion which was reported in fraud losses last year. We, of course, know the real number is far higher.

By the way, between 2021 and 2024, Congressional Budget Office (CBO) reported scams and fraud were up 110 percent under the CFPB's oversight. So doubling down on failure is pretty much the last thing that we are going to do to solve this crisis.

Fraud and scam roundtables have been held by our committees, telecom companies have been invited in, tech platforms, hosting tele-town halls with community banks, working with us, with our U.S. Attorney General's Office, as well as State Attorney General's offices.

We have been working at it since the beginning of this Congress, and we are making progress, and we are as determined to fight this crisis situation as you folks clearly are.

To Ms. McKune, I would like to start the questioning with you. By the way, great testimony. I really appreciated what you had to say.

From your experience, how effective is consumer education in preventing scams before money ever leaves a customer's account?

Ms. MCKUNE. Thank you for the question.

We see this as an essential piece of how we are protecting our consumers. We absolutely have to have educated consumers because many times, as Mr. Rust has noted, there is so much shame involved in admitting that you have been scammed. That is one layer of the problem.

The other is that these are—they call it social engineering for a reason. These are manipulations of people's vulnerabilities and the things that they worry most about.

If we are in a position where they are not going to answer our questions, they are not going to tell us what is happening, the best tool we have, really, the very first tool has to be fundamental understanding and sophistication in consumers about the risks of fraud. It is why we are really supportive of an all-of-government approach and a top-down consumer education movement, because we do really see it as the essential first step.

Mr. MEUSER. So all of government, all of private sector are very holistic, and that is definitely the strategic plan.

Mrs. Dempsey as well, great opening testimony. Thank you so much.

When a customer walks into one of your branches after they have been deceived online, what options do you and other community banks realistically have to stop loss at that point?

Mrs. DEMPSEY. Well, if they have already sent it there is not a lot that we can do at that point, if it has been outside our bank and what we have done.

Ms. McKune as well, just education, the ongoing education of trying to inform them before of when they are coming in to get the money, of being bold enough—like I mentioned, we have got really strong relationships with our customers, so we know them. Our tellers do an incredible job of really just asking questions—"What are you doing with this? Why do you need to take this much out of the bank?"—and things of that nature.

I know we have talked, too, about just an overall approach. So I want to highlight like with the ICBA, one thing we did with the U.S. Postal Inspection Service was to come up with an in-branch handout to give to consumers to educate them and to start a conversation on fraud and scams. So hundreds of thousands of those have been given out at almost a thousand banks and so anything that we can do to bring attention to it and to stop it before it happens.

Mr. MEUSER. Thank you very much.

Mr. McDade as well, excellent testimony.

How important would it be if social media platforms were required to verify advertisers and quickly remove scam ads once they have been reported?

A number of you have referenced the SCAM Act. The SCAM Act will certainly be requiring this of social media companies with penalties that are appropriate.

Go ahead, please.

Mr. MCDADE. I would say it is essential. The reality is these scams originate outside of our bank's control environment, they, most of them—I believe there is a study out of Britain that said 80 percent of the scams that they were seeing in that country they alleged came from Meta as a platform.

So when you take a look at that, we need to do something in order to have correct accountability in those places.

Mr. MEUSER. Okay. Excellent.

You know, I was in New York City, we visited BNY Mellon and JPMorgan's fraud and scam prevention centers. They are spending

millions, if not, with a "B," billions, on tracking and preventing scams.

Do you believe telecom providers and social media platforms are making the same level of investment to stop scams?

Mr. MCDADE. Unfortunately, they are not. While we do try to partner as well as we can with the telecoms and the social media, the reality is since they do not bear any of the liability, they do not bear the responsibility as far as they are concerned.

We have actually reached out to telecoms and asked them to have a "this is a scam email alert" on the phone just like you get "this is spam." The truth of the matter is they are regulated for spam, they are not regulated for scams, and so we have not gotten the response that we need.

Mr. MEUSER. Thank you.

I am almost out of time. Mr. Schuster, I had a question for you on what else, regarding preventing scam calls and texts from reaching consumers in the first place, but I am out of time. Perhaps we can talk about that offline.

I yield back, Mr. Chair.

Chairman BARR. The gentleman from Massachusetts, Mr. Lynch, is recognized.

Mr. LYNCH. Thank you very much, Mr. Chairman.

First of all, I want to thank the panelists. You have all been terrific and thank you for your work on this issue.

Honestly, I feel, though, that if this is Consumer Protection Week, we should probably drape the Capitol in black crepe because consumer protection is dead, it really is, based on what has been happening here lately.

I honestly think that President Trump is ushering in the golden age of fraud with all the actions that he has done.

Since January 2025—this is just his second term. We are not going to touch the stuff in his first term—the Trump Administration has undertaken unprecedented efforts to undermine the Consumer Financial Protection Bureau through systematic dismantling—the one agency that is charged with protecting the consumer.

This is the one agency that Congress has identified and structured to protect the consumer. Yet the administration moved immediately to effectively shut down CFPB by declaring its funding structure unconstitutional, unlawful, in November 2025, and it refused to seek additional funding from the Federal Reserve, which just would have starved the agency.

On February 10, 2025, Acting Director Russell Vought issued a stop-work order instructing all CFPB employees to stop protecting American consumers and to not perform their work tasks as the agency announced it would run out of money by early 2026.

The administration also moved to terminate nearly all CFPB staff. This is during the Department of Government Efficiency (DOGE) scourge. They canceled—the administration canceled about $100 million in employment contracts for those employees whose job it was to protect consumers.

Although a Federal judge eventually ordered a pause of those actions in February, many of those employees, who were very valuable, very capable and qualified employees, were placed on admin-

istrative leave and were unable to perform their duties, and eventually many of them left because they felt they had such uncertainty.

Remember, this is the agency that CFPB returned $19.7 billion from people who had scammed consumers, put that money back in Americans' pockets, $5 billion, the amount of money that CFPB had imposed on civil penalties on companies and individuals that violate the law.

Especially, and this is key, we do a lot of work at Fort Hood and some of these big bases, they recovered $363 million in monetary relief resulting from 30 million public enforcement actions that involved harm to servicemembers.

They are not being paid enough to begin with, and these are a lot of young families that are barely making it; and also veterans, including six enforcement actions for violation of the Military Lending Act.

So that is what Trump is eliminating, that ability.

This is all—I am not even going to get into what the Trump family themselves are doing. This is the same time—so the Trump family launched Liberty Financial. This is Trump's sons, all of them, also Zach Witkoff, who is Steve Witkoff's son. They launched that at the same time that the Trump Administration eliminated the crypto crimes enforcement unit.

So he goes into business in crypto, and then he eliminates the crypto crimes enforcement unit. Tell me that is not connected and he dropped enforcement on a ton of actions at the SEC and the CFPB. He rolled back a bunch of rules curbing scams at payday lenders. He delayed the implementation of the fiduciary duty rule.

So he has done all of this to, as I say, to launch the golden age of fraud, removing enforcement.

So, Mr. Rust, what do you think about our ability to conduct current enforcement actions and guardrails in order to protect consumers? Where do we stand right now given all that I have said?

Mr. RUST. Well, it is true, it has been gutted, in so many ways.

I think in the brief amount of time I want to highlight how they are not helping servicemembers, which is one of the things the Bureau has always done. There has not been a visit to a military installation. There have been no monitoring reports to prevent scams targeting servicemembers and veterans. No annual report to understand priorities or complaint trends. The dropping of the Navy Federal Credit Union enforcement action, and the MoneyLion settlement pennies on the dollar. The most recent Reduction in Force (RIF) plan would have left the Office of Servicemember Affairs with no staff.

Mr. LYNCH. Thank you.

Thank you, Mr. Chairman. I yield back.

Chairman BARR. The gentleman's time has expired.

The gentlewoman from California, Mrs. Kim, is now recognized for 5 minutes.

Mrs. KIM. Thank you. Thank you, Chairman, for holding this hearing and I want to thank our witnesses for joining us today.

You know, in California, we are in the golden age of fraud with more types of fraud than Baskin-Robbins has flavors of ice cream.

Sadly, our Governor, Gavin Newsom, has done little to stop this crisis.

That is why I introduced the No More SCAMS Act that would create a Federal strike force dedicated to investigating fraud involving Federal dollars, bringing fraudsters to justice, and clawing back stolen taxpayer dollars for the American people.

I believe that we can learn a lot from the private sector and the great tools that you have deployed to combat fraud and scams to put the consumers first.

So I going to ask the first question to you Mr. McDade.

How do banks leverage third-party fraud tools to work across financial institutions and prevent scams and fraud?

Mr. MCDADE. Thank you for the question.

Banks the size of EverBank, we are a mid-sized regional bank, we do have a national presence, and we do have a presence specifically in California.

When we look at it; we do not necessarily have the resources to build our own AI constructs. We do not have the data scientists, necessarily, to do that.

So we depend on groups like LexisNexis, Early Warning Services (EWS), and other consortium-based tools to help us find the fraud signals out in the environments that they touch, report those signals to us so we can collaborate back and forth, and risk rate transactions and risk rate potentially fraudulent customers that are trying to break into the fraud ecosystem, and they are essential partners for us.

Mrs. KIM. That is exactly why we need to do something similar at the Federal level to streamline those efforts, right?

Then there are third-party fraud fighters who are successful because they can dialog with different financial institutions and connect it from pieces of puzzle.

Similarly, the task force that I envision through this legislation, the No More SCAMS Act, will be able to utilize the resources of the different Federal agencies and combine both the manpower and the information to track down those frauds.

Mr. McDade, how does improved coordination across agencies can stop scams in the banking system?

Mr. MCDADE. So we are calling for a national task force on fraud, and we think that one of the things we need is alignment across all the different agencies and all the different law enforcement entities.

The reality is, as I talked about in my testimony, when a fraud report is made by a consumer there is not necessarily a specific agency that they can point to pick it up because different agencies have different mandates, and then you have the local law enforcement.

I would say something to be done in that direction would be the GUARD Act that is being talked about, which is similar to the High Intensity Drug Trafficking Areas (HIDTA) program that I worked with as a prosecutor where we allow the Federal resources to partner with the State resources for these $20,000 to $50,000 scams that are hitting our banks that do not rise to the level of Federal prosecution, but are multi-jurisdictional, and so there is a difficulty with law enforcement approaching them.

Mrs. KIM. Thank you. Thank you.

You know, one type of financial fraud that I particularly focus on is the credit repair scams. I serve as the co-chair of the Financial Literacy and Wealth Creation Caucus, and I have seen the damage of those scams on consumers who are exploited by false promises involving their credit scores.

To that end, I am co-leading the Ending Scam Credit Repair Act to help end those types of scams and prevent bad actors from stealing money from hardworking American families.

So, Mr. Chairman, I would like to ask for unanimous consent to submit this letter that I got from the American Financial Services Association emphasizing the need to end—the need for this type of legislation.

Chairman BARR. Without objection.

[The information referred to can be found in the appendix on page 150.]

Mrs. KIM. I also have another letter from SIFMA to also——

Chairman BARR. Without objection.

[The information referred to can be found in the appendix on page 152.]

Mrs. KIM. Thank you very much.

Let me shift gears now. I want to also focus on romance scams and the work that is being done to cracking down on them.

I was proud to lead the effort to have the Treasury Department identify romance scam facilitators in Cambodia as money laundering entities. While that was a great step in the right direction to crack down on bad actors, we must also focus on ways to prevent those scams at the point of attack as well.

So, Ms. McKune, how are credit unions like Park Community using methods such as consumer education to prevent romance scams before—before—the money gets taken?

Ms. MCKUNE. This is part of our broad consumer education efforts. We are aware that romance scams are a problem.

Not to make light in any way of the ways our members are victimized, but Keanu Reeves might need to come before the committee. Keanu Reeves is someone who gets pulled out as people posing as Mr. Reeves, and we have had multiple members who believed that they were in a relationship with Mr. Reeves.

We know about them, we try to educate our members, and we move as quickly as we can when we see the signs of those.

Chairman BARR. The gentlelady's time has expired.

The gentleman from Texas, Mr. Green, is now recognized.

Mr. GREEN. Thank you, Mr. Chairman.

Mr. Chairman, the better name or better title for this hearing would be "Fighting Fraud on the Front Lines: Challenges and Opportunities for Trump and the Trump Administration to Engage in Corruption."

Let me start by asking unanimous consent that certain articles be introduced into the record.

The first is styled "Melania Trump's meme coin architects accused of pump-and-dump fraud in lawsuit."

The second one is styled "Trump meme coin down 96% as Bitcoin and meme coins slide," and I have a third. The third one has to

do with Kristi Noem. "Firm Tied to Kristi Noem Secretly Got Money From $220 Million DHS Ad Contracts."

Allow me to go through these articles very quickly. I think they paint a picture of corruption.

The first is in The Guardian, the one styled—did I get unanimous consent, Mr. Chair, to introduce my articles? Mr. Chairman? Mr. Chairman?

Chairman BARR. Without objection.

[The information referred to can be found in the appendix on pages 155–168.]

Mr. GREEN. Thank you.

The article from The Guardian styled "Melania Trump's meme coin architects accused of pump-and-dump fraud in lawsuit," reading it in various portions we find the language: The $MELANIA coins were released for just a few cents each on 19 January, the day before Donald Trump was inaugurated. I am paraphrasing, and then it goes on to say: Within hours, this coin's price soared to $13.73.

Then it goes on to read: However, it then collapsed almost as quickly and is now worth about 10 cents, less than 1 percent of its peak price. It goes on to add that at its peak it was worth $45.47. It goes down to $5.79.

The article goes on to indicate: The Trump family has pocketed more than $1 billion—more than $1 billion—in pretax profits from several cryptocurrency-related products over the past 12 months.

Then we have the second one, "Trump meme coin down 96 percent as Bitcoin and meme coins slide." Reading in part from the article: "Last February, the coin's market capitalization stood at $3.5 billion, already well below its $14.5 billion peak on the eve of his second inauguration. Today, it has fallen to $1.78 billion."

Then it reads, in part, that the scale—they are talking about a pump-and-dump scheme here, it talks about the scale of this pump-and-dump scheme involving at least 15 cryptocurrencies, included the $MELANIA currency. It indicates that, of course, the coin is down 96 percent in this scam.

Now, let us move over to Secretary Noem. Secretary Noem, the article is styled: "Firm Tied to Kristi Noem Secretly Got Money From $220 Million DHS Ad Contracts." $143 million has gone to a mysterious LLC Delaware company created just days before it was awarded a deal.

The corruption that this administration has imposed upon the public, pocketing big money from pump-and-dump schemes, is unbelievable. When you read it, it is almost like reading a corruption story in some magazine.

I am going to yield back the balance of my time, Mr. Chairman, but I think that these things have to be further investigated.

Chairman BARR. The gentleman's time has expired.

The gentleman from South Carolina, Mr. Timmons, is now recognized.

Mr. TIMMONS. Thank you, Mr. Chairman and thank you to the witnesses for being with us today.

Financial fraud and scams are becoming one of the fastest-growing financial crimes facing Americans. Increasingly, these schemes are carried out by large-scale criminal networks operating over-

seas, often using sophisticated technology, coordinated infrastructure, and social engineering tactics that target Americans at scale.

As these operations evolve, financial institutions are often the first line of defense. Banks and credit unions are responsible for detecting suspicious activity, protecting their customers, and coordinating with law enforcement.

As fraud networks grow more complex and increasingly operate across borders, it raises serious questions about whether our current legal and regulatory frameworks are fully equipped to support the institutions working to stop these crimes.

Mr. McDade, in your testimony you noted that the FBI received more than 850,000 IC3 complaints involving over $16 billion in losses last year alone.

Based on your experience, both in the banking sector and as a former prosecutor handling complex fraud cases, would you agree that a significant portion of these modern scams are being conducted by large organized criminal operations operating in foreign jurisdictions?

Mr. MCDADE. Yes. The evidence is very clear that is happening. We get phone spoofs that are coming from overseas phones. Our bank is a primary digital bank, and we are able to often detect whether or not things are coming from overseas, and a large number of the fraud accounts that we see attempting to be open are from overseas.

There has been some very strong media coverage about that, The New York Times and The Economist showing scam compounds as massive, organized crimes larger than, in some cases, the drug trade in Southeast Asia and Africa.

Mr. TIMMONS. Thank you for that.

How do these operations differ from the more traditional fraud schemes we saw a decade or two ago?

Mr. MCDADE. Well, the reality is they are able to leverage at scale some of the techniques that used to be done piecemeal. They are gathering data from data breaches, they are gathering data from, as I said earlier, publicly available resources, such as the PPP lending site, and they are cross-referencing those, we believe, using artificial intelligence and machine learning, in order to create profiles that they are able to know a great deal about the individual customers they are approaching and take a focused effort with knowledge of how that customer normally transacts in order to fool them into believing that they are a trusted source as they approach them.

Mr. TIMMONS. So technology is largely to blame for the more sophisticated version of scams and frauds?

Mr. MCDADE. The scammers and fraudsters are using technology at scale is what we are observing.

Mr. TIMMONS. Is it fair to say that 20, 30 years ago, if you were to engage in this, it is going to be on a small scale, and you are going to have a higher propensity of getting caught by law enforcement?

Mr. MCDADE. I would say that it is much easier for them to avoid law enforcement because they can have anonymity online as they are doing this work.

Mr. TIMMONS. Well, it is not that they have anonymity. It is that we do not have the jurisdiction to pursue criminal charges and hold them accountable. Is that fair?

Mr. MCDADE. That is fair to say. When they are multinational, it is much more difficult to have prosecution.

Mr. TIMMONS. We can use the resources that we have to address attribution. It is not easy, but we have the ability to figure out who is engaging in certain scams. Is that correct?

Mr. MCDADE. At times it is possible that we can point to specific areas and specific individuals overseas.

Mr. TIMMONS. Do you know of any other area of crime that the U.S. Government just does not enforce? I mean, we have the ability to hold these people accountable in foreign jurisdictions, we just do not do it.

I mean, is that fair to say? I mean, we could figure out who is engaging in $16 billion worth of fraud, and we could hold them accountable, but we choose not to.

Mr. MCDADE. I cannot really speak to the specific efforts that are happening there, but I would agree that everybody agrees that more attention to fraud and scams in a more significant approach is absolutely necessary.

Mr. TIMMONS. Obviously education to make Americans protect themselves better is huge. I mean, everyone is susceptible to a certain degree. I just feel like the Federal policies should address that and should say, if you are engaging in organized crime, we are going to attempt to arrest you. If you are in a nonextradition country, we are going to use other tools in our toolbox.

The President's favorite word is tariffs, and he could say: All right, we are going to make the victims whole, and then we are going to impose tariffs to recoup our losses, or you can just give us the person that committed the crime.

I mean, so we do have the ability to hold these people accountable and to make the victims whole, but we choose not to do that. I mean, we could hold organized crime accountable in Eastern Europe and Southeast Asia, but we choose not to. Is that fair?

Mr. MCDADE. I would just say that banks would welcome any resources the Federal Government wanted to bring to bear to help stop this epidemic of fraud and scams.

Mr. TIMMONS. Well, I could not agree—we need to get our act together.

I appreciate you all being here today.

With that, I yield back.

Mr. MCDADE. Thank you.

Chairman BARR. The gentleman yields.

The gentleman from Wisconsin, Mr. Fitzgerald, is recognized.

Mr. FITZGERALD. Thank you, Chairman.

Thank you for being here today. I know it has been a couple hours, so I appreciate that.

So I was at a bank in my district last week, a prominent bank in southeastern Wisconsin, and we had a very good discussion with staff at that bank about fraud and then we had credit unions this week in DC. So I talked to a number of people about it.

I do not think this topic came up. Maybe it did. Maybe it touched on it this morning. I have got Judiciary going on as well but in

both of those instances there was a component of this which is related to family members that actually are part of the fraud, or sometimes bilking, for the most part the targets are adults, and it is another family member is having a discussion about one of their accounts. It is not until kind of the front line, which is oftentimes the person working at the credit union or the bank that is in a teller position, that kind of realizes something is not right.

So I was just wondering if I could just get a thought on the family aspect of this, and certainly law enforcement. I mean, they do not want to get involved in any of these fraud-related scams that are nationwide, but when it includes a family member it is even more hands-off, is what I am being told. I am wondering if you believe that is the case.

Mrs. Dempsey?

Mrs. DEMPSEY. Not in our community and that falls, for us, it sounds like, more under Adult Protective Services when we see family members that are taking advantage of an elderly grandparent or aunt or uncle or things of that nature. I am not sure if that is what you are implying.

Mr. FITZGERALD. Yes. That is what the discussion is about.

Mrs. DEMPSEY. Yes, or a caregiver that has gotten control as an authorized signer on their account or something of that nature.

So for us in Tennessee we have also got very good laws to help us with elder abuse and prevention and protection. So we have a good relationship with our law enforcement and Adult Protective Services when we recognize that and see it happening.

Mr. FITZGERALD. Very good.

Mr. McDade?

Mr. MCDADE. I would echo the fact that we would approach adult and family services within our eldercare program when we do detect something that could indicate someone is being taken advantage of by somebody close to them.

There are processes to do that. It is usually through the State's Attorney General's Office in the various States that we do business in, and we regularly make those reach-outs when it is appropriate.

Mr. FITZGERALD. Very good.

Ms. McKune?

Ms. MCKUNE. I want to note that one of the things that I think can give law enforcement some trepidation is how very complex these situations are.

They rely heavily on us to try to unwind and figure out what is going on. We lean into our tellers in our branches when they have good relationships and know some of the dynamics, but it is unquestionably true that vulnerable folks are vulnerable, and that can be family members, that can be people they have designated as powers of attorney, et cetera.

So we do as much as we can to package the information to say this is why we believe this is what is going on.

Mr. FITZGERALD. Very good.

Mr. Schuster?

Mr. SCHUSTER. Thank you.

It is a great question. I think you are hearing that financial institutions are doing a lot to identify these frauds. They are many

times, on the front lines, identifying where there are family fraud, potential elder abuse, and reporting that, and that helps.

This is not something that the CFPB is doing. This is financial institutions themselves and having laws that restrict their ability to stop these types of things are where there are impediments to continuing to help consumers.

Mr. FITZGERALD. Very good.

Mr. Rust, I do not know if you have a comment on that topic.

Mr. RUST. I agree with much of what has been said, but I also want to emphasize the size of reporting. If the amount is only $2,000 or $3,000, which is still plenty, that needs to be routed up to law enforcement.

I think a whole-of-government approach to public infrastructure surrounding complaints. People should not have to know which agency they should complain to. That information should be, if it ends up in the wrong agency, shared with the correct agency with the kind of customer service relationship work that the Bureau has always shown.

Mr. FITZGERALD. Very good.

Thank you so much. I yield back, Chairman.

Chairman BARR. The gentleman yields back.

I would like to thank all of our witnesses for their testimony today. We have come to the end of this hearing.

Without objection, all members will have 5 legislative days to submit additional written questions for the witnesses to the chair. The questions will be forwarded to the witnesses for their response.

Witnesses, if you could please respond no later than April 9 if you do get such written questions.

Again, I want to thank all of our witnesses for your excellent testimony and contributions. I think we heard a lot of good recommendations here to deal with this multi-billion-dollar problem for the American people and hopefully we can make progress. Thanks for all the great work that you all do protecting your customers and the American people.

This hearing is now adjourned.

[Whereupon, at 12:02 p.m., the subcommittee was adjourned.]

APPENDIX

MATERIALS SUBMITTED FOR THE RECORD

american securities association
America's Voice for Main Street's Investors

March 5, 2026

The Honorable Andy Barr
Chairman, Subcommittee on Financial Institutions
Committee on Financial Services
U.S. House of Representatives
Washington, DC 20515

The Honorable Bill Foster
Ranking Member, Subcommittee
Committee on Financial Services
U.S. House of Representatives
Washington, DC 20515

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

Dear Chairman Barr and Ranking Member Foster:

On behalf of the American Securities Association[1] (ASA), thank you for convening this important hearing[2] to exam how financial institutions, regulators, and law enforcement can better combat fraud and protect America's investors and savers.

ASA represents American financial services firms that provide small and mid-cap businesses with access to capital and advise hardworking Americans on how to create and preserve wealth, with a mission to promote trust and confidence among investors and support competitively balanced capital markets.

I. General.

In written comments to the House Select Committee on the Chinese Communist Party dated May 16, 2023,[3] ASA described how the Chinese Communist Party (CCP) has "methodically exploited the U.S. capital markets while sponsoring cybercriminals that steal the personal and financial information of Americans," imposing "heavy costs on American investors, the U.S. economy, and the integrity of the U.S. capital markets."

[1] ASA is a trade association that represents the retail and institutional capital markets interests of regional financial services firms who provide Main Street businesses with access to capital and advise hardworking Americans how to create and preserve wealth. ASA's mission is to promote trust and confidence among investors, facilitate capital formation, and support competitively balanced capital markets. This mission advances financial independence, stimulates job creation, and increases prosperity. ASA has a geographically diverse membership base that spans the Heartland, Southwest, Southeast, Atlantic, and Pacific Northwest regions of the United States.

[2] House Financial Services Subcommittee on Financial Institutions hearing titled, "Fighting Fraud on the Front Lines: Challenges and Opportunities for Financial Institutions, available here:
https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=411032

[3] ASA Submits letter to the Select Committee on the Chinese Communist Party, May 16, 2023, available here:
https://files.constantcontact.com/ca98267e701/50657974-148a-4259-8f99-e6211115594b.pdf.

Additionally, in testimony prepared for the United States Senate Special Committee on Aging,[4] ASA further detailed the risks the CCP poses to American investors and senior savings and outlined steps Congress can take to prevent further investor harm.

II. Fraud, Foreign Exploitation, And Senior Investors.

In previous written and oral testimony, ASA explained that while the free flow of capital can promote economic growth and strengthen the rule of law, it can also be exploited by authoritarian regimes and sophisticated fraudsters in ways that directly harm American investors.

To that end, we note that foreign adversaries and their proxy companies have used the U.S. capital markets to fund forced labor, human rights abuses, cyber-operations, and other activities hostile to American interests, with many of them turning out to be frauds.

This committee can address the Chinese company fraud risk that exists directly through Variable Interest Entity (VIE) companies and indirectly by including these companies in mutual and exchange-traded funds. Without such protections, American investors harmed by these companies will find they have little to no legal redress.

III. Front-Line Fraud.

Recent congressional work on "pig butchering" scams illustrate how fraudsters weaponize technology, social engineering, and cross-border structures to separate victims from their life savings. In a widely covered hearing, Representative Raja Krishnamoorthi highlighted a case[5] in which scammers instructed a victim to liquidate assets and purchase physical gold bars as "payment," demonstrating the extreme and manipulative tactics used to steal from seniors and retail investors.

CCP-linked cyber actors and fraud networks target the personal and financial information of American investors, making them more vulnerable to these kinds of sophisticated schemes. Taken together, the Krishnamoorthi example and ASA's prior work show that Americans can do "everything right" under existing rules and still lose their life savings when criminals exploit technological, jurisdictional, and regulatory gaps.

---

[4] Testimony of Christopher A. Iacovella, President & CEO, American Securities Association, Hearing Entitled "Financial Aggression: How the Chinese Communist Party Exploits American Retirees and Undermines National Security." United States Senate Special Committee on Aging and the United States House Select Committee on the Strategic Competition between the United States and the Chinese Communist Party, available here: https://www.congress.gov/119/meeting/house/118132/witnesses/HHRG-119-ZS00-Wstate-IacovellaC-20250409.pdf.

[5] Rep. Krishnamoorthi highlights scam factories, available here: https://abc7chicago.com/post/illinois-us-rep-raja-krishnamoorthi-cites-abc7-team-report-push-stop-pig-butchering-scams-congressional-hearing/16296267/#:~:text=He%20showed%20a%20recent%20I,compelled%20to%20engage%20in%20scams.%22.

IV. Recommendations for this Subcommittee to Strengthen Fraud Protections.

We offer the following recommendations to help protect American investors—particularly seniors—from fraud and foreign exploitation of our capital markets.

- Strengthen public-private partnerships. ASA urges closer collaboration between government agencies and financial firms, especially on cybersecurity and fraud detection, arguing that a "reset" in this relationship is needed to combat sophisticated fraud and state-sponsored schemes.
- Incentivize businesses to report fraud. ASA recommends that Congress and regulators design incentives so firms are rewarded—not punished—for promptly reporting fraud and threats. This will contribute to corporate responsibility and market transparency.
- Create an anonymous reporting portal for scams. ASA would like you to think about adopting a secure portal where regulated firms can anonymously report trends or specific fraudulent activity targeting their firm or customers, giving regulators more timely intelligence on new scams without fear of retribution.
- Focus on emerging threats like AI-driven fraud. In comments to the House Financial Services Committee, we highlighted the rise of AI-generated fraud and schemes tied to foreign state actors (such as the Russian and Chinese government) as growing risks to American families and investors.
- Continue to use hearings like this to push policy changes. ASA has submitted letters and comments to House Financial Services subcommittees in hearings specifically examining tools and techniques to combat fraud, outlining policy options for Congress and regulators to better protect households from investment scams.
- Advance bipartisan legislation such as the No China in Index Funds Act and make certain the Foreign Investment Guardrails to Help Thwart (FIGHT) China Act is implemented to prevent American retirement and savings capital from financing CCP-controlled or CCP-backed companies that pose fraud, cyber, and national-security risks.
- Review how large-scale regulatory data-collection initiatives, like the SEC Consolidated Audit Trail or CAT, expose investors to fraud and cyber risk. This Congress must not allow regulators and market utilities to collect and retain, in any form, the personal and financial information of Americans that could be turned against them.

By incorporating these recommendations, the Subcommittee can strengthen the broader U.S. response to fraud on the front lines. It will also reinforce a clear message to investors and markets alike: protecting America's seniors, working families and savers from fraud—whether domestic or foreign in origin—is a bipartisan priority and a core obligation for financial institutions, regulators, and policymakers.

american securities association
America's Voice for Main Street's Investors

V. Conclusion.

Thank you again for your leadership in convening this timely hearing and for your commitment to protect investors from nation states and bad actors intent on defrauding Americans. Please do not hesitate to contact us if we can be of further assistance to the Subcommittee.

Sincerely,

Christopher A. Iacovella

Christopher A. Iacovella
President & CEO
American Securities Association

American Securities Association
1455 Pennsylvania Ave. NW, Suite 400
Washington, D.C. 20004

AmericanSecurities.org
@amersecurities

202.621.1784

AFSA
AMERICAN FINANCIAL SERVICES ASSOCIATION

March 4, 2026

The Honorable Andy Barr
Chairman
Subcommittee on Financial Institutions
Committee on Financial Services
U.S. House of Representatives
Washington, DC 20515

The Honorable Bill Foster
Ranking Member
Subcommittee on Financial Institutions
Committee on Financial Services
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Barr and Ranking Member Foster:

On behalf of the American Financial Services Association (AFSA),[1] thank you for conducting the hearing entitled, "Fighting Fraud on the Front Lines: Challenges and Opportunities for Financial Institutions." We appreciate the opportunity to highlight a particular financial scam, one perpetrated by certain credit repair companies, which costs American families thousands of dollars annually and perpetuates billions of dollars in fraud. Certain legal and regulatory barriers hinder the ability of financial institutions to mitigate credit repair fraud, and so we encourage the members of the Subcommittee on Financial Institutions to support H.R. 306, the "Ending Scam Credit Repair Act" or ESCRA. This legislation will protect consumers from illegitimate entities that falsely promise to rebuild their credit histories while charging expensive monthly fees, but allow legitimate businesses to serve their customers. The ESCRA would also decrease fraud.

As the Federal Trade Commission (FTC) warns, "Credit repair scams also frequently target financially distressed consumers who are having credit problems. These operations lure consumers to purchase their services by falsely claiming that they will remove negative information from consumers' credit reports even if that information is accurate."[2] The FTC has brought many enforcement actions against these bogus credit-related services. Credit repair scammers charge consumers expensive monthly fees, but if the negative information they are disputing is accurate, it cannot be permanently removed from a consumers' credit history. Therefore, consumers are paying large sums of money, but not receiving any benefit – quite a scam.

Sometimes, credit repair scammers achieve a brief period of success. When financial institutions are overwhelmed with duplicative disputes, the disputed information may be removed from the consumers' credit history temporarily, while the financial institution investigates the dispute. During the time the disputed information is temporarily removed, in a type of fraud known as "credit washing," consumers' apply for credit for which they would not otherwise qualify. Credit washing hurts consumers themselves, who now have more debt they cannot afford to repay. It also hurts creditors.

---

[1] Founded in 1916, the American Financial Services Association (AFSA) is the national trade association for the consumer credit industry, protecting access to credit and consumer choice. AFSA members provide consumers with many kinds of credit, including traditional installment loans, mortgages, direct and indirect vehicle financing, payment cards, and retail sales finance.

[2] https://www.ftc.gov/news-events/topics/consumer-finance/debt-relief-credit-repair-scams.

Credit washing is adding to the ever-growing fraud problem for vehicle finance companies and banks. In 2025, the vehicle finance industry faced an estimated $9.2 billion in fraud loss exposure.[3] This number continues to grow, with experts estimating that it will reach $10.4 billion in 2026.[4] While there are many types of vehicle fraud, credit washing is a large part of the problem. In August of 2025, suppressions of credit data reached their highest levels ever, up 504% in 18 months.[5]

The reason for this dramatic increase is that sophisticated technologies give scammers the ability to commit fraud faster than the financial institutions can combat it. AI platforms are generating millions of false and duplicative credit disputes in an attempt to overwhelm financial institutions' systems.

To reduce credit repair scams and credit washing fraud, as well as help address affordability concerns, Congress should pass H.R. 306. The ESCRA would impose a six-month moratorium on payments to credit repair companies, closing the loophole that encourages credit washing. It would also require disclosure, letting consumers know that they are paying for a service that they could do themselves. In addition, the ESCRA would ensure that consumers receive the promised services by requiring that a credit repair lawyer be able to be contacted. Perhaps most importantly, credit repair scammers would be prohibited from sending repeated, false disputes.

We appreciate your efforts in combatting the rise of fraud in financial transactions, costing American families billions of dollars each year. The ESCRA is a necessary step in countering fraud, and we urge the committee to pass this needed legislation. Please contact me at cwinlow@afsamail.org with any questions.

Sincerely,

Celia Winslow

Celia Winslow
President and CEO
American Financial Services Association

---

[3] https://pointpredictive.com/press-releases/2025-auto-lending-fraud-trends-report-9-2-billion-industry-risk/.
[4] https://www.autofinancenews.net/allposts/risk-management/dealers-say-up-to-24-of-auto-loan-defaults-caused-by-fraud/.
[5] https://www.transunion.com/faq/what-is-credit-washing.

sifma
Invested in America

March 5, 2026

The Honorable Andy Barr
Chairman
Subcommittee on Financial Institutions
Committee on Financial Services
U.S. House of Representatives
Washington, DC 20515

The Honorable Bill Foster
Ranking Member
Subcommittee on Financial Institutions
Committee on Financial Services
U.S. House of Representatives
Washington, DC 20515

Re: U.S. House Subcommittee on Financial Institutions Hearing Entitled: Fighting Fraud on the Front Lines: Challenges and Opportunities for Financial Institutions

Dear Chairman Barr and Ranking Member Foster,

The Securities Industry and Financial Markets Association ("SIFMA") commends the Financial Institutions Subcommittee of the House Financial Services Committee for holding this important hearing to examine the challenges and opportunities for financial institutions. Fraud targeting investors is one of the fastest-growing threats to our financial system, and we value the Committee's leadership in exploring how everyone can work together to protect investors across the country. SIFMA appreciates the opportunity to submit our comments for the record.

At SIFMA, protecting investors has been a longstanding core focus of our advocacy and policy work. For over 15 years, we have collaborated with our members, academic experts, and policymakers at both the state and federal levels to advance policies, rules, regulations, and statutes that enhance protections and empower financial professionals to detect, prevent, and report financial exploitation. SIFMA supported the first state law that gave firms the capability to halt suspicious financial transactions, and we later supported a federal law enabling broker-dealers nationwide to place temporary holds on transactions when fraud is suspected. We have also developed and promoted tools including trusted contact forms, temporary holds on transactions, and safe harbor laws that allow firms to act when they see red flags. Today, a growing number of states have enacted similar investor protection laws that extend to broker-dealers, and several other states are currently working to develop a similar path. Consistent with this commitment, SIFMA has advanced policies and initiatives aimed at protecting investors from fraud and scams. For example, SIFMA has recently focused on working with policymakers and investigative agencies to ensure open lines of communication between financial institutions and

sifma
Invested in America

investigators – which has proven to be a key driver of positive outcomes in attempted fraud cases.

We also work closely with victim support services organizations, research institutions, and other nationwide partners. A few months ago we sponsored NAPSA's Financial Exploitation Prevention Summit, which brought together Adult Protective Services ("APS") professionals, researchers, bankers, law enforcement, investors, regulators, and government officials to discuss strategies for combating financial exploitation.

As part of these broader efforts, SIFMA, alongside our member firms and partners, developed a Senior Investor Protection Toolkit, available for free on our website. This comprehensive resource provides tools and educational materials to help older investors safeguard their finances.

Another key SIFMA-backed initiative is HelpVul (Helping Vulnerable Adults), developed in partnership with NAPSA, EverSafe, and Hunter College with support from the U.S. Department of Justice. This innovative online reporting platform enables financial institutions to securely report suspected exploitation to APS and state securities regulators, standardizing and enhancing investigations of financial abuse across agencies. Already active in several states and dozens of institutions, HelpVul allows real-time referrals, secure communication, and case tracking. It also incorporates digital forensic tools to detect patterns of exploitation.

In the past couple of years, we have seen a great increase in the international fraud trends that are negatively impacting our clients' savings. To that end, we have created an Anti-Fraud Task Force at SIFMA that will look at the issues more broadly than in the past. While we have previously focused on seniors and vulnerable individuals, this Task Force will work against all forms of fraud. We have brought together operational experts, state law experts, anti-money laundering experts, compliance experts and other financial fraud experts. We are committed to creating a network of peers to problem solve and find ways to get ahead of financial fraud.

Safeguarding investors is a shared responsibility. On behalf of the financial services industry, SIFMA stands ready to work together with policymakers, law enforcement, advocates, and families to protect investors from fraud and scams and enhance investor protections. Protecting investors from such attacks is a complex and rapidly evolving challenge — particularly given the rise of AI — one that demands coordinated action across sectors and the broader community. We remain committed to pursuing solutions that leverage legislation, regulation, education, technological innovation, and collaborative partnerships to address this growing threat.

sifma
Invested in America

We thank the Subcommittee for its leadership in convening this hearing and look forward to continuing our efforts to strengthen investor protections and combat the evolving threats of financial fraud.

Sincerely,

Lisa Bleier
Head - Wealth Management, Retirement and State Government Relations
SIFMA

CC: Chairman French Hill and Ranking Member Maxine Waters

The Guardian

Melania Trump's meme coin architects accused of pump-and-dump fraud in lawsuit

By Guardian staff and agency

October 23, 2025



Melania Trump speaks in Washington DC on 10 October 2025.

Andrew Leyden/Zuma Press Wire/Shutterstock

The designers of a cryptocurrency launched by the US first lady, Melania Trump, in January were accused in court filings on Tuesday of orchestrating a pump-and-dump scheme.

The $MELANIA coins were released for just a few cents each on 19 January, the day before Donald Trump was inaugurated as US president.

In addition to $MELANIA, Donald Trump launched $TRUMP a few hours before his inauguration.

Within hours, the $MELANIA coin's price soared to $13.73.

However, it then collapsed almost as quickly, and is now only worth about 10 cents – less than 1% of its peak price. $TRUMP traded at a peak of $45.47 and now goes for $5.79, according to Coin Market Cap.

The plaintiffs say the coin's creators organized the operation knowing that the digital currency's value would plummet.

Melania Trump herself is not named in the lawsuit. The plaintiffs said they did not believe she was "culpable," but accused the crypto companies of using her and other familiar faces as "window dressing" for their crimes.

In newly filed court papers, investors accuse the executives of the Meteora cryptocurrency exchange platform, on which $MELANIA was initially traded, of setting up a scheme that allowed them to indirectly purchase large quantities of the virtual coin.

Their accomplices then quickly resold these digital currencies, pocketing substantial profits while causing the price to plummet, according to documents filed on Tuesday in Manhattan federal court.

The allegations concerning $MELANIA have been added to legal proceedings involving several other cryptocurrencies, which began in April. Meteora did not immediately respond to a request for comment.

The Trump family has pocketed more than $1bn in pre-tax profits from several cryptocurrency-related products and companies over the past 12 months, the Financial Times reported last week.

Fast Company

Trump meme coin down 96% as Bitcoin and meme coins slide

By Chris Morris

February 9, 2026

On January 19, 2025, someone paid $75.35 to buy a Trump meme coin. Today, assuming that same investor held the cryptocurrency, the investment has lost 96% of its value.

The crypto market has been more volatile than usual in recent weeks. Last week alone saw daily swings of as much as $10,000 in Bitcoin, the leading digital currency, pushing it down to nearly $60,000, a level not seen since 2024.

Bitcoin has since recovered somewhat, though it is still hovering near $70,000, well below its $122,000 high last October. But as mainstream cryptocurrencies continue to give investors whiplash, meme coin holders have fared even worse.

The Trump coin, in midmorning trading on Monday, stood at $3.39, according to CoinMarketCap. The Melania coin, which once traded as high as $13.73, is down roughly 99%, changing hands for about 12 cents.

The drop in the Trump coin comes roughly a year after it began to lose investor support following Trump's inauguration. Last February, the coin's market capitalization stood at $3.5 billion, already well below its $14.5 billion peak on the eve of his second inauguration. Today, it has fallen to $1.78 billion.

Nonpolitical meme coins have also seen steep declines. Dogecoin, which once flirted with $1 per coin, is now trading at just over 9 cents. That represents a 25% decline year to date and a 68% drop since last September.

Shiba Inu now costs $0.000006060, meaning that buying 1,650 coins today would cost just under one cent—a 20% drop from its highs last October. Losses over the past week span the broader meme coin market: Pepe fell 13%, Bonk dropped 16%, Pudgy Penguins declined 20%, and Pippin slid 35%. (No, we didn't make any of those names up, and no, it's not surprising if you haven't heard of several of them.)

Crypto's turbulence comes amid broader market instability in 2026. Wall Street has experienced its own roller-coaster ride, and even precious metals have been volatile, with silver prices swinging between $71 and $115 since January 1.

What makes crypto's ups and downs particularly noteworthy, though, is the financial stakes held by President Donald Trump's two eldest sons. Eric Trump and Donald Trump Jr. co-founded American Bitcoin, a publicly traded Bitcoin mining and treasury management company, in March of last year. (The stock has fallen from $7.40 per share when it began trading to $1.28 in midday trading on Monday.)

Eric Trump, Donald Trump Jr., and 19-year-old Barron Trump are also co-founders of World Liberty Financial, a crypto company that is now generating more revenue for the family than the Trump real estate business. The Wall Street Journal calculates that the company has brought in at least $1.4 billion for the Trump family since Trump's reelection.

The sons of Trump special envoy Steve Witkoff and Commerce Secretary Howard Lutnick also operate businesses with crypto interests. A White House spokesperson told the Journal that there are no conflicts of interest, as the ventures are run independently by the politicians' sons.

Meme coins have always been risky investments. All too often, they're rug pulls—get-rich-quick schemes in which one entity sees significant returns, but investors are left with useless holdings. And while they might be tied to a pop culture phenomenon or a person, there's no guarantee that there's any formal relationship between the two.

That could be the case with the Melania meme coin. Last October, a lawsuit was filed alleging that the coin's backers orchestrated a large-scale pump-and-dump scheme involving at least 15 cryptocurrencies, including $MELANIA. The complaint alleged that first lady Melania Trump was used as "window dressing for a crime engineered by Meteora and Kelsier."

"Neither Melania Trump nor her representatives knew the project was part of a systemic fraud, and they would not have agreed to any use of her name had they known the truth," the suit read.

ProPublica

Firm Tied to Kristi Noem Secretly Got Money From $220 Million DHS Ad Contracts

By Justin Elliott, Joshua Kaplan and Alex Mierjeski

November 14, 2025



Secretary of Homeland Security Kristi Noem films an ad at Mount Rushmore.

Tia Dufour/Department of Homeland Security

On Oct. 2, the second day of the government shutdown, Homeland Security Secretary Kristi Noem arrived at Mount Rushmore to shoot a television ad. Sitting on horseback in chaps and a cowboy hat, Noem addressed the camera with a stern message for immigrants: “Break our laws, we’ll punish you.”

Noem has hailed the more than $200 million, taxpayer-funded ad campaign as a crucial tool to stem illegal immigration. Her agency invoked the "national emergency" at the border as it awarded contracts for the campaign, bypassing the normal competitive bidding process designed to prevent waste and corruption.

The Department of Homeland Security has kept at least one beneficiary of the nine-figure ad deal a secret, records and interviews show: a Republican consulting firm with long-standing personal and business ties to Noem and her senior aides at DHS. The company running the Mount Rushmore shoot, called the Strategy Group, does not appear on public documents about the contract. The main recipient listed on the contracts is a mysterious Delaware company, which was created days before the deal was finalized.

No firm has closer ties to Noem's political operation than the Strategy Group. It played a central role in her 2022 South Dakota gubernatorial campaign. Corey Lewandowski, her top adviser at DHS, has worked extensively with the firm. And the company's CEO is married to Noem's chief spokesperson at DHS, Tricia McLaughlin.



"My marriage is one thing and work is another. I don't combine them," said DHS Assistant Secretary for Public Affairs Tricia McLaughlin, who is married to Strategy Group CEO Ben Yoho.

Tricia McLaughlin via Instagram

The Strategy Group's ad work is the first known example of money flowing from Noem's agency to businesses controlled by her allies and friends.

Government contracting experts said the depth of the ties between DHS leadership and the Strategy Group suggested major potential violations of ethics rules.

"It's corrupt, is the word," said Charles Tiefer, a leading authority on federal contract law and former member of the Commission on Wartime Contracting in Iraq and Afghanistan. He said that the Strategy Group's role should prompt investigations by both the DHS inspector general and the House Oversight Committee.

"Hiding your friends as subcontractors is like playing hide the salami with the taxpayer," Tiefer added.

Federal regulations forbid conflicts of interest in contracting and require that the process be conducted "with complete impartiality and with preferential treatment for none."

"It's worthy of an investigation to ferret out how these decisions were made, and whether they were made legally and without bias," said Scott Amey, a contracting expert and general counsel at the watchdog group Project on Government Oversight.

The revelations come as the amount of money at Noem's disposal has skyrocketed. The so-called Big Beautiful Bill granted DHS more than $150 billion, and Noem has given herself an unusual degree of control over how that money is spent. This summer, she began requiring that she personally approve any payment over $100,000.

Asked about the Strategy Group's work for DHS, McLaughlin, the agency spokesperson, said in an interview, "We don't have visibility into why they were chosen."

“I don’t know who they’re a subcontractor with, but I don’t work with them because I have a conflict of interest and I fully recused myself,” she said. “My marriage is one thing and work is another. I don’t combine them.” Her husband, Strategy Group CEO Ben Yoho, didn’t respond to questions.

A woman with blonde hair poses with a man wearing a brown houndstooth suit jacket for a selfie on a plane.

In a written statement, DHS said, “DHS has no involvement with the selection of subcontractors.” They added that the Strategy Group does not have a direct contract with the agency, saying “DHS cannot and does not determine, control, or weigh in on who contractors hire.”

Contracting experts said that agencies can and do sometimes require that subcontractors be approved by officials. It’s not clear how much the Strategy Group has been paid.

This is not the first time that the Strategy Group has gotten public money through a Noem contract. As governor of South Dakota in 2023, her administration set off a scandal by hiring the Ohio-based company to do a different ad campaign, paying it $8.5 million in state funds. While the state said the contract was done by the book, a former Noem administration official told ProPublica that Noem quietly intervened to ensure the Strategy Group got the deal. ProPublica granted some people anonymity to discuss the deals because of their sensitivity.

The firm also paid up to $25,000 to one of Noem’s closest advisers in South Dakota, previously unreported records show. (The adviser, 28-year-old Madison Sheahan, now serves at DHS as the second-in-command of Immigration and Customs Enforcement. Sheahan didn’t respond to questions about why she was paid.)

The DHS ad that the company filmed at Mount Rushmore has aired during "Fox & Friends" in recent days. Executives from the Strategy Group traveled to the shoot and hired subcontractors to fill out the film crew, according to records and a person involved in the campaign. The ad's aesthetic sits somewhere between a political campaign ad and a Jeep commercial as Noem tells would-be immigrants to "come here the right way.

"From the cowboys who tamed the West to the titans who built our cities," Noem says, as images of Trump Tower in Chicago and Trump raising his fist after the assassination attempt last year flash on the screen, "America has always rewarded vision and grit." Noem continues: "You cross the border illegally, we'll find you."

The ad is the latest in a campaign that Noem debuted in February, just a few weeks after she took charge of DHS. "Any delay in providing these critical communications to the public will increase the spread of misinformation, especially misinformation by smugglers," the agency wrote, explaining why it was skipping the competitive bidding process normally required for government contracts. The initial ads featured Noem thanking Trump for securing the border.

The contracts total $220 million so far, leading the DHS ad budget to triple in the most recent fiscal year, according to Bloomberg. The lion's share of ad contracts is typically used to buy TV airtime or spots on social media. Advertising firms make money by taking an often-hefty commission. Federal records show the contracts have gone to two firms. One is a Republican ad company in Louisiana called People Who Think, which has been awarded $77 million.

But the majority of the money — $143 million — has gone to a mysterious LLC in Delaware. The company was created just days before it was awarded the deal.

Little is known about the Delaware company, which is called Safe America Media and lists its address as the Virginia home of a veteran Republican operative, Michael McElwain. McElwain has long had his own advertising company (separate from the Delaware one), but there's little evidence that firm could handle a nine-figure federal contract on its own: It reported just five employees when it received COVID-19 relief money a few years ago.

How, where and to whom Safe America Media doled out the $143 million is unknown. Any subcontractors hired to do work on the DHS ads are not disclosed in federal contracting databases.

The office funding the ad contracts is listed as the DHS Office of Public Affairs, which is run by McLaughlin, contract records show. McLaughlin married Yoho, the Strategy Group CEO, earlier this year.

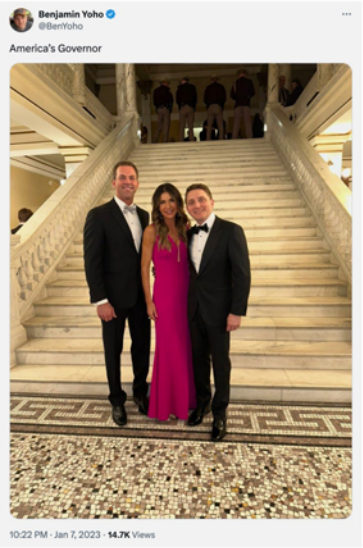
In its statement, DHS said the agency does its contracting "by the book" and the process is run by career officials. "It is very sad that Pro Publica would seek to defame these public servants," DHS added.

Asked about why the agency chose Safe America Media, DHS said, "The results speak for themselves: the most secure border in American history and over 2 million illegal aliens exiting the United States." McElwain and People Who Think didn't respond to questions.

Yoho was still in college when he first served as campaign manager for a U.S. congressman. Now, at 38 years old, he's a national player in the cutthroat industry of political advertising. Federal election records show tens of millions in payments to his firm during the 2024 election cycle, coming from dozens of Republican congressional candidates. And Noem has proved a particularly lucrative client.

Lewandowski brought Yoho into Noem's inner circle back in South Dakota, according to two people familiar with the matter, putting the young consultant in charge of the ad side of her 2022 gubernatorial reelection campaign. Noem had a more than $5 million advertising

budget for the race, records show. After she won in a landslide, Yoho, who has called Noem a friend, came to South Dakota to attend her inauguration ceremony. He sat off to the side of the stage, next to Lewandowski. (Lewandowski didn't respond to a request for comment.)



Yoho shared a photo of himself with Noem and her husband, Bryon, at Noem's 2023 inauguration in South Dakota.

Benjamin Yoho via X

By then, Yoho's next big project with Noem was already in the works. In late 2022, Noem was quietly preparing to launch another sprawling ad campaign — only this time, the money would come from state coffers. The stated goal was to encourage workers to move to South Dakota. The upcoming contract opportunity wasn't public yet, but Yoho was already involved in planning the campaign, according to records first reported by Sioux Falls Live.

Then on Jan. 12, 2023, Yoho's company registered to do business in South Dakota under the name Go West Media. The next day, the contract opportunity went live.

Seven companies submitted proposals for the project. Then the pressure from above set in, according to a former Noem administration official involved in the process.

The former official said a top Noem aide told them the governor would be angry if Yoho's company didn't win the contract. "He was very direct: 'She wants to do it,'" they said. Contemporaneous text messages reviewed by ProPublica corroborate that senior Noem administration officials pushed for Yoho to get the contract. Eventually, he did. (In its statement, DHS denied that Noem influenced the process.)

Noem starred in Yoho's ads herself, dressing up as a dentist, a plumber and a state trooper as she touted her state's growing economy. Exactly how much Yoho and the Strategy Group made off the $8.5 million deal is unclear. Some of the money was used to purchase spots on Fox News, including one during a Republican presidential debate. Some of the money appears to have gone back to South Dakota — into the bank account of another of Noem's top advisers.

Sheahan, now the second-in-command at ICE, was paid up to $25,000 by Go West in 2023 for "consulting," according to a financial disclosure document Sheahan later filed. At the time, Sheahan was serving as both the operations director for Noem as governor and the political director for Noem's campaign work, according to a copy of her 2023 resume obtained by ProPublica. Her responsibilities included coordinating "daily logistics and operations" for Noem and her team, the resume said. She also managed the "relationship with high level donors" to American Resolve, Noem's network of outside political groups.

As his firm received millions from the South Dakota state government, Yoho separately continued to work for Noem in other capacities. He worked under Lewandowski on the publicity campaign for Noem's 2024 memoir, according to a person familiar with the matter. (The book became famous for including an anecdote about Noem shooting her dog.)

The Strategy Group also received a stream of payments for social media consulting and media production work over the last few years from Noem's American Resolve PAC. Federal election records show the PAC made its last payment to Yoho's company this February, a couple weeks after Noem took her post as the head of DHS.

BANK POLICY INSTITUTE

Statement for the Record from the Bank Policy Institute

Before the U.S. House Financial Services Committee, Financial Institutions Subcommittee

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

March 5, 2026

The Bank Policy Institute (BPI) appreciates the opportunity to provide input to the Subcommittee on the hearing "Fighting Fraud on the Front Lines: Challenges and Opportunities for Financial Institutions."[1] BPI member institutions are deeply committed to protecting customers and the integrity of the U.S. financial system from fraud and scams. Fraud and scams have grown in both scale and sophistication, driven in large part by digital platforms, mobile communications and emerging technologies such as artificial intelligence. Banks are often the first to detect suspicious activity and the first place to which consumers turn when they realize they have been victimized, yet most scams begin outside the banking system: on social media, messaging apps, online marketplaces and telecom networks. A durable solution therefore requires a coordinated, whole-of-ecosystem approach that aligns incentives, clarifies responsibilities and prioritizes scam prevention at the source.

The Changing Fraud Landscape

Criminals increasingly exploit social media, messaging platforms and telecom channels to impersonate trusted institutions, distribute fraudulent content and conduct large-scale phishing and spoofing campaigns. Deepfake audio and video, synthetic identities and convincing fake websites and apps make it easier than ever for fraudsters to deceive consumers, including vulnerable populations and older Americans. Banks invest heavily in analytics, authentication and customer education to detect and disrupt these attacks, but they cannot control the design and policing of the platforms where scams originate.[2] [3]

Regulators and policymakers have recognized the growing threat and the need for more consistent expectations across sectors. At the same time, the current framework for fraud and scam prevention remains fragmented, with different agencies overseeing discrete portions of the problem and relatively limited mechanisms for real-time information sharing across industries. Clarifying the responsibilities, encouraging cross-sector collaboration and updating outdated rules can significantly improve consumer protection without undermining access to fast, convenient payments.

Principles for an Effective Anti-Fraud Framework

[1] The Bank Policy Institute is a nonpartisan public policy, research and advocacy group that represents universal banks, regional banks and the major foreign banks doing business in the United States. BPI produces academic research and analysis on regulatory and monetary policy topics, analyzes and comments on proposed regulations, and represents the financial services industry with respect to cybersecurity, fraud and other information security issues.

[2] Federal Bureau of Investigation. (2025). FBI releases annual Internet Crime Report. https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report

[3] Federal Trade Commission. (2025, March). New FTC data show big jump in reported losses to fraud: $12.5 billion in 2024. https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024

BPI believes that a national strategy is needed to combat fraud and scams. This strategy should be grounded in the following principles:

- Prevention efforts should focus on the channels where scams originate, especially social media, messaging, online advertising and telecom networks.
- Responsibilities should be clearly allocated across sectors so that every link in the chain—banks, telecom providers, social media platforms, regulators and law enforcement—has meaningful obligations commensurate with its role and capabilities.
- Real-time, cross-sector information sharing should be encouraged and protected, building on the successful models used in cybersecurity.
- Banks acting in good faith to pause or scrutinize suspicious transactions should have appropriate legal protections and regulatory flexibility.
- The national strategy should coordinate efforts by the federal government, prioritize high-impact initiatives and avoid duplicative or conflicting mandates.

Policy Recommendations

To advance these principles, BPI recommends that Congress and the relevant agencies focus on five concrete areas of reform, consistent with the comprehensive analysis presented in BPI's recent Fraud and Scam Prevention Playbook.[4]

1. Strengthen obligations for social media and digital platforms

Congress and regulators should establish baseline requirements for social media, online marketplaces and other digital platforms to verify advertisers and merchants, quickly remove fraudulent content and disrupt obvious scam-recruitment and impersonation schemes. "Know Your Merchant"-style standards for paid advertising and marketplace listings would help prevent fraudulent promotions before they reach consumers.[5] Clear timelines for removing reported scam content, combined with reporting obligations for repeat offenders, would better align incentives across the ecosystem.

BPI has endorsed the bipartisan Safeguarding Consumers from Advertising Misconduct (SCAM) Act, introduced in the House by Representatives Dan Meuser and Lou Correa, which would require online platforms to verify advertisers, ban paid scam ads, establish rapid takedown obligations and strengthen FTC and state enforcement authority.[6] This legislation represents an important step toward holding digital platforms accountable for fraudulent advertising and complements the broader anti-fraud framework outlined in this statement.

2. Enhance telecom and messaging network responsibilities

Telecom providers and messaging platforms are critical gatekeepers for phone calls and text messages used in scam campaigns. These firms should be expected to authenticate high-risk traffic, block known scam numbers and spoofed domains, and provide consumers with accessible tools to report suspected scams in real time.[7]

---

[4] Bank Policy Institute. (2026, February). Fraud and Scam Prevention Playbook.
[5] The Guardian. (2024, December 2). Meta to force financial advertisers to be verified in bid to prevent celebrity scam ads targeting Australians. https://www.theguardian.com/technology/2024/dec/02/meta-to-force-financial-advertisers-to-be-verified-in-bid-to-prevent-celebrity-scam-ads-targeting-australians
[6] U.S. House of Representatives. (2026, February 11). H.R. 7548, Safeguarding Consumers from Advertising Misconduct Act. https://www.congress.gov/bill/119th-congress/house-bill/7548
[7] Google. (2025). How we're using AI to combat the latest scams. https://blog.google/innovation-and-ai/technology/safety-security/how-were-using-ai-to-combat-the-latest-scams/

Regulators should facilitate greater sharing of known scam indicators, such as numbers, URLs and message templates, across carriers and with banks, enabling earlier detection and intervention before consumers complete a fraudulent payment.

3. Provide safe harbors and regulatory flexibility for banks to protect customers
Banks should have clear authority and a safe harbor to delay or block transactions when they reasonably suspect fraud or a scam, especially where the pattern of activity or customer behavior is inconsistent with past usage. Modernizing rules that govern funds availability and check processing—while preserving prompt access to funds for routine transactions—would allow banks to better tailor controls to emerging fraud typologies without fear that well-intentioned protective measures will later be second-guessed.[8] When banks act in good faith based on reasonable indicators of risk, they should not face additional liability for attempting to protect customers.

4. Facilitate real-time, cross-sector information sharing
Congress should encourage and, where appropriate, provide safe harbor protections for cross-sector information sharing related to fraud and scams. Building on established cybersecurity information-sharing frameworks, banks, telecom providers, social media companies and law enforcement should be able to exchange timely indicators of fraud and scam activity, consistent with privacy and consumer protection laws, to more quickly identify and dismantle emerging schemes.[9] Clarifying antitrust and liability concerns in this context would help remove barriers that currently deter proactive collaboration.

5. Establish a National Anti-Scam Strategy
Finally, BPI supports the creation of a coherent federal strategy to combat fraud and scams, led by a central office or coordinator charged with aligning agency efforts and engaging the private sector. A National Anti-Scam Strategy could set measurable goals, prioritize high-impact initiatives and ensure that policies with respect to fraud and scams that govern payments, telecom, online platforms and financial services are mutually reinforcing. Elevated federal leadership would also help integrate consumer education campaigns, victim support resources and law enforcement efforts targeting domestic and international scam networks.

Conclusion

Banks are on the front lines of protecting consumers from fraud and scams, but they cannot solve this problem alone. Most scams begin on platforms and networks outside the banking system, and the most effective interventions will prevent criminals from ever reaching their victims. By aligning incentives across sectors, clarifying responsibilities and enabling real-time collaboration, Congress and the relevant agencies can dramatically strengthen protections for American households and businesses while allowing legal commerce to flourish.

BPI and its member institutions stand ready to work with anyone to develop and implement a comprehensive, practical framework to reduce fraud and scams. We appreciate the Subcommittee's attention to this critical issue and the opportunity to contribute our perspective.

---

[8] Bank Policy Institute. (2025, September). Statement for the Record: Fraud in Focus. https://bpi.com/wp-content/uploads/2025/09/BPI-Statement-for-the-Record-Fraud-in-Focus.pdf
[9] Cybersecurity Information Sharing Act of 2015, Pub. L. No. 114-113.

Responsible Data Alliance

March 4, 2026

VIA ELECTRONIC SUBMISSION

The Honorable Andy Barr
Chairman
Subcommittee on Financial Institutions
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Bill Foster
Ranking Member
Subcommittee on Financial Institutions
U.S. House of Representatives
Washington, D.C. 20515

Re: House Financial Services Committee's Subcommittee on Financial Institutions Hearing Entitled "Fighting Fraud on the Front Lines: Challenges and Opportunities for Financial Institutions"

Dear Subcommittee Chairman Barr and Ranking Member Foster:

The Responsible Data Alliance ("RDA"), an association of leading risk data providers, is pleased to submit the following letter related to the House Financial Services Committee's ("Committee") Subcommittee on Financial Institutions ("Subcommittee") hearing entitled "Fighting Fraud on the Front Lines: Challenges and Opportunities for Financial Institutions."[1] Our members are dedicated to protecting financial institutions, consumers, businesses, and government entities from fraud, identity theft, and other illicit activities while streamlining consumer-initiated transactions. We appreciate the opportunity to provide our perspective on the serious challenges that fraud poses to financial institutions and illustrate how those institutions rely upon responsible third-party data and service providers to combat fraud.

I. Fraud is a pervasive and growing challenge that contributes to significant annual losses for institutions across the financial sector.

Financial institutions routinely partner with third-party data and service providers that provide highly accurate and efficient data-driven tools and services that are essential to combating fraud and identity theft. Financial institutions depend on these third-party offerings to protect their customers from fraud, identity theft, scams, and other illegal activities.[2] Access to these services is critical as fraud presents an increasing and material challenge for financial institutions of all sizes. According to the Federal Trade Commission ("FTC"), in 2024 alone, there were more than 1.1 million reports of identity theft received through the FTC's identity theft portal.[3] In that same year, consumers reported losing more than $12.5 billion to fraud—a figure 25 percent greater than the year before.[4] Broader estimates that include institutional

[1] *See* House Financial Services Committee's Subcommittee on Financial Institutions, "Fighting Fraud on the Front Lines: Challenges and Opportunities for Financial Institutions," March 5, 2026, *available* here.
[2] *See, e.g.*, Emilio Cividanes, *Attacks on 'data brokers' ignore their key role in consumer protection*, American Banker (March 2, 2026), available here.
[3] *See* Federal Trade Commission, Press Release, *New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024* (March 10, 2025), available here.
[4] *Id.*

losses are substantially higher; for example, a 2024 Nasdaq report estimated total U.S. fraud loss in 2023 at "more than $138 billion."[5]

Fraud comes in a multitude of forms, each of which fuels its own significant losses for both consumers and institutions. For example, scams account for approximately 36 percent of overall fraud losses and negatively impact financial institutions across various industries.[6] Synthetic identity fraud likewise accounts for significant losses.[7] Synthetic fraud presents unique challenges in an era of online transactions, where interactions are remote, identities can be fabricated from fragments of real and fake information, and there is no face-to-face contact to reliably confirm that a person is who they claim to be.[8] These challenges have led to a higher proportion of synthetic fraud attacks involving credit card applications, which carry enormous costs that can follow consumers for years to come.[9] The result is a multi-faceted fraud problem that negatively impacts a growing number of consumers and institutions year over year.

Fraud's costs extend far beyond the initial direct fraud loss, with many financial institutions reporting that fraud also results in significant downstream impacts such as diminished consumer trust, increased compliance and regulatory response workloads, and costly resource reallocation to prepare for future fraud risks.[10] One industry survey demonstrates that, when accounting for these downstream impacts, U.S. financial services bear an average of $5.75 in total cost for every $1 of fraud loss.[11] These costs are felt across the entirety of an impacted financial institution, with two-thirds of industry respondents reporting that fraud affects at least four business areas.[12] This pervasive fraud problem is exacerbated as fraudsters grow in sophistication and leverage new technologies, such as deepfakes and other AI-powered schemes, to evolve their operations.[13]

II. Access to data and services from third-party providers is vital to combat fraud and identity theft affecting financial institutions and consumers.

Responsible third-party data and service providers play a critical role in helping financial institutions mitigate and manage fraud across industries. For instance, financial institutions use third-party data services to verify consumer identities, detect suspicious activities, and stop fraudsters from misusing personal information. Third-party providers thus help to increase trust when customers bank online, open accounts, or engage in other important transactions central to their financial freedom and security. Consumers, particularly those in vulnerable populations more frequently targeted by fraudsters, benefit directly from more secure transactions. Robust

---

[5] Nasdaq Verafin, *The Impacts of Financial Crime on the U.S. Economy* 4 (2024), available here.
[6] *See* LexisNexis Risk Solutions, *LexisNexis True Cost of Fraud Study 2025 North America: Financial Services & Lending* 9 (2025), available here; *see also* Socure, *Socure Identity Risk Insights: Defining and Solving the Elusive Challenge of First-Party Fraud* 7–8 (2023), available here (describing widespread fraud losses among a variety of financial institutions, including community banks and credit unions).
[7] *See* LexisNexis Risk Solutions at 6–7.
[8] *Id.* at 7.
[9] *See* SentiLink, *The SentiLink Fraud Report: Identity Fraud Rates & Trends 1H 2025* 18 (2025).
[10] *See* LexisNexis Risk Solutions at 3–4.
[11] *See id.* at 8.
[12] *See id.* at 4.
[13] *See* SentiLink at 35–36.

fraud prevention services based on responsible data use allow financial institutions to leverage expertise and technology to enhance fraud prevention and identity management efforts that better protect both financial institutions and consumers themselves. From local community banks and credit unions to the largest banks in the country, financial institutions' ability to address potential fraud efficiently using third-party data and services has never been more important, as bad actors perpetrate fraud using increasingly sophisticated techniques and operations.[14]

Effective fraud prevention requires continued, pre-transaction access to the third-party data that helps ensure these services are highly accurate, detecting fraud while minimizing false positives and negatives. Data-driven solutions depend on the existence and continued availability of third-party data within the broader data ecosystem. For example, the identity verification services that underpin modern fraud prevention tools rely upon the existence of historical data about a given consumer. By drawing upon this historical data from third-party providers, these tools can assess nearly instantaneously whether a given transaction aligns with an individual's past financial behavior and identity patterns, or whether the transaction could be an indication of potential fraud—for example, because the individual is trying to access their online bank account from a state where they do not live.

The exceptions in Section 502(e) of the Gramm-Leach-Bliley Act ("GLBA") are crucial for enabling third-party data and service providers to provide the tools and services that protect financial institutions and consumers from fraud. Preserving these exceptions is essential to ensuring that core consumer protection activities related to fraud and identity theft prevention can persist. Without the ability to responsibly access and use data from third parties for fraud prevention purposes, financial institutions would not be able to ascertain potential fraud as accurately or efficiently. And when fraud goes undetected, it can cause significant harms to institutions and consumers alike. Continued access to third-party data from responsible providers is critical to enhance the common defense and protection of both consumers and financial institutions from fraud.

* * *

As the Subcommittee considers how today's financial institutions address fraud, we encourage you to recognize the immense opportunities for fraud and identity theft prevention that are enabled through the safe and responsible use of third-party data and services. Our members are committed to working with you to ensure that critical data uses that protect financial institutions and their consumers are preserved. Please feel free to contact us at info@responsibledata.org with any questions.

Sincerely,

The Responsible Data Alliance

CC: Committee Chairman French Hill

[14] *See, e.g.*, *id.* at 35–39; LexisNexis Risk Solutions at 13–15.

ALTA
American Land Title Association

March 4, 2026

The Honorable Andy Barr
Chairman
House Committee on Financial Services
Subcommittee on Financial Institutions
Washington, DC 20515

The Honorable Bill Foster
Ranking Member
House Committee on Financial Services
Subcommittee on Financial Institutions
Washington, DC 20515

Dear Chairman Barr, Ranking Member Foster, and Members of the Subcommittee:

On behalf of the American Land Title Association (ALTA), I appreciate the opportunity to submit this letter for the record for the hearing entitled *Fighting Fraud on the Front Lines: Challenges and Opportunities for Financial Institutions*. ALTA represents an industry comprised of more than 17,000 title companies operating in every county across the nation and employing more than 150,000 professionals. Title professionals are involved in nearly every real estate transaction, residential and commercial, where large dollar transfers and sensitive personal and financial information create attractive targets for criminals. Title professionals take immense pride in their work to promote confidence in the real estate market and safeguard consumers against fraud.

The work of title professionals is centered around protecting homebuyers. Title professionals work extensively to identify and resolve risks that may not be found in the publicly available record, such as undisclosed liens, unpaid taxes, and other title defects. These issues may not be apparent at the closing table, but when they surface, they can delay transactions, cause financial harm, or result in costly legal disputes for homeowners who lack effective safeguards. This curative work can also include detecting fake deeds and seller impersonation fraud before a transaction closes, ensuring that homebuyers' savings and lenders' collateral are protected. Title professionals are dedicated to combating fraud and protecting the largest investment that Americans often make in their lives.

Despite the extensive curative work of title professionals, fraud remains one of the most expensive and damaging threats to homeowners. Today, fraud accounts for approximately 21 percent of total claim dollars paid by title insurers, with average losses exceeding $143,000 per claim. This risk exposure is even greater in refinance transactions, where average fraud-related

losses exceed $207,000.[1] Wire fraud, primarily carried out through business email compromise schemes, remains a persistent threat in any real estate transaction, accounting for the second most common method by which funds are reported lost across all fraud schemes.[2] In these schemes, criminals attempt to divert closing funds by sending fraudulent wire instructions to buyers, lenders, or settlement agents. A 2024 title industry survey found that half of all companies reported experiencing wire fraud attempts.[3] Recent research also suggests that at least 25 percent of consumers are targeted by criminals during a given real estate transaction, resulting in nearly 5 percent becoming fraud victims. Compared to current or former homeowners, first-time buyers are three times more likely to fall victim to these fraud schemes.[4]

Title professionals regularly partner with law enforcement and financial institutions to detect and report fraudulent or illicit activity occurring at the crossroads of the housing market and financial system. The title industry has also invested in technology and educational campaigns to ensure that homebuyers do not fall prey to these crimes. In 2025, ALTA announced new policy endorsements allowing new and existing homeowners to add coverage that offers protection against forgery of a deed or mortgage, including the legal costs necessary to defend them if fraud occurs. These endorsements expand consumer protection beyond the moment of closing by addressing risks that emerge after the purchase. ALTA also updated its industry Best Practices to strengthen fraud prevention by enhancing staff training, tightening oversight of notaries and signing agents, and establishing clear protocols for responding to suspected fraud. Together, these ongoing measures underscore the industry's commitment to protecting consumers from devastating financial losses.

In the context of real estate transactions, reliable and comprehensive safeguards are essential to ensure that consumers are protected against fraud and other unknown risks. Title insurance is regulated at the state level by departments of insurance to ensure policies and rates are fair, non-discriminatory, and adequately protect consumers. Recently, there has been a trend in the market to promote alternatives to title insurance, such as attorney opinion letters (AOLs). AOLs are often marketed to homebuyers as "equally protective and less expensive" when compared to title insurance, however that is not the case. Unlike title insurance, these alternatives do not provide ongoing protection against undiscovered risks like fraud, nor do they include a duty to defend the policyholder in the case of litigation. Unfortunately, providers of these alternatives do not currently need to comply with the same state-based regulations as title insurance that ensure transparency of coverage and pricing. Due to this lack of regulation, differences in coverage may not always be clear to homebuyers, increasing the risk that they opt for these alternatives without fully understanding the protections they may forgo. Recently, some state officials have echoed this concern, including the Virginia Commissioner of Insurance, who wrote in a recent Administrative Letter that, "the gap in coverage may leave consumers without

---

[1] Milliman, *Analysis of Claims and Claims-Related Losses in the Land Title Insurance Industry*, commissioned by the American Land Title Association, November 2025, https://www.alta.org/file/2025-Analysis-of-Claims-and-Claims-Related-Losses-in-the-Land-Title-Insurance-Industry.pdf; Milliman, *Analysis of Claims and Claims-Related Losses in the Land Title Insurance Industry*, May 2024, https://www.alta.org/media/pdf/240517-analysis-of-claims-and-claims-related-losses-in-the-land-title-insurance-industry.pdf

[2] Federal Bureau of Investigation, *Internet Crime Complaint Center (IC3) 2024 Annual Report*, May 2024, https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

[3] American Land Title Association, Seller Impersonation Fraud Study Report, August 2023, https://www.alta.org/file/Seller-Impersonation-Fraud-Study-Report.pdf

[4] CertifID, State of Wire Fraud 2025, https://www.certifid.com/state-of-wire-fraud

protection that they believe they purchased."[5] It is imperative that policymakers at the state and federal level act to ensure that consumers are not deceived into putting their largest investment, their home, at risk.

To address these concerns and ensure consistent consumer protections, ALTA urges swift consideration and enactment of H.R. 3206, the Protecting America's Property Rights Act, introduced by Representatives Andrew Garbarino (R-NY) and Vicente Gonzalez (D-TX). This legislation would require that all products being marketed and utilized to insure title risk on federally backed mortgages are properly regulated at the state level. Enactment of H.R. 3206 would ensure that consumers receive the reliable, regulated protection they expect when purchasing a home.

Thank you for the opportunity to submit this letter for the record. ALTA and its members look forward to continuing to work with Congress to combat fraud, strengthen consumer protections, and promote confidence in the real estate market.

Sincerely,

Chris Morton
Chief Executive Officer
American Land Title Association

[5] Virginia State Corporation Commission, Bureau of Insurance, Administrative Letter 2025-05: Gap in Coverage Attorney Opinion Letters, September 30, 2025, https://www.alta.org/file/Virginia-Insurance-Commission-Letter-on-Alternatives-09092025

Question 1

Could you expand on why it is so important for the Federal Reserve to enforce timeliness in correspondence in cases like this, and what the practical consequences are for community banks in Tennessee when that enforcement role is removed?

Response:

The Federal Reserve's enforcement of timeliness in correspondence ensured that each party was responsive to the other during fraud disputes. When we pursued our breach-of-warranty claim in 2022 on behalf of a small business customer who had approximately 15 to 20 checks stolen from the mail, totaling almost $600,000, the Federal Reserve mediated the dispute from the initial claim through to resolution. We pursued our case citing UCC law, with the mediation of the Fed, and were able to recover 100 percent of the funds, though it still took approximately six months.

Without that enforcement role, the situation is very different for community banks. After the Federal Reserve removed itself from the process following the initial return and response, a payor bank like ours must pursue its claim directly with the bank of first deposit. The larger institution is not held to any timeliness standard and may not respond at all. We experienced this in a separate case involving a $118,000 cashier's check that was stolen and altered. For eight months, we tried to make contact with the large depositing bank. We wrote letters, called every number we could find, and reached out to the Tennessee Bankers Association for help locating a contact. When we finally identified someone who could supposedly help, he responded to our first email and then went silent when he learned what the issue concerned.

The practical consequences for community banks in Tennessee are real. Without the Federal Reserve's enforcement of timely correspondence, larger institutions have no incentive to be responsive to our legitimate claims. Community banks are left absorbing losses that should rightfully reside with the depositing bank. Given our smaller asset sizes, these losses make a fundamental impact on our ability to serve our local communities. A large bank with hundreds of billions or more than a trillion dollars in assets can more easily absorb fraud losses. For a $225 million asset bank like ours with 44 employees and three branches, fraud losses disproportionately impact us. It is doubtful that we would have been able to recover the $600,000 in the first case had we been operating under today's rules.

I would also note that the Federal Reserve Board recently published a request for information on the future of its check collection and processing services, raising the possibility that these services could be discontinued. Federal Reserve Vice Chair for Supervision Michelle Bowman has recognized the importance of these services and issued

a statement opposing the RFI. I urge this committee to support the continuation of Fed check services, which are the primary or sole check processing provider for many community banks and play a valuable role in dispute resolution.

Question 2

Could you briefly talk about how a more streamlined, standardized interbank dispute resolution process could help level the playing field and ensure that community banks with legitimate claims aren't left holding the bag when fraud occurs?

Response:

Community banks report that large financial institutions often reject fraud claims even when we provide significant documentation. Contacts at larger institutions 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 we have legitimate claims.

As I noted in my testimony, an appropriately tailored resolution process could provide more standardized, timely, and effective resolution of interbank disputes. It would also provide a clearer framework for evaluating breach-of-warranty claims, reducing the ability of larger institutions to exploit ambiguous rules to shift losses onto community banks.

Regulation CC should also explicitly define liability allocation for specific fraud scenarios, particularly for altered checks and forged endorsements. In the case of our $118,000 cashier's check, the depositing bank claimed the check was "counterfeit," which would put liability on our bank, while we maintained it was "altered," which would put liability on the depositing bank. The check number, amount, date, bank logo, address, signature, and other characteristics were all the same. Only the payee had been changed. ICBA and community banks have been asking the UCC Permanent Editorial Board to revisit and modernize the definitions of "counterfeit" and "altered," which were written before today's digital alteration techniques existed. Clear definitions would help level the playing field.

An effective dispute resolution process should also require full transparency from all parties. As I noted in my testimony, all parties should be held to full transparency. In the cashier's check case, we learned ten months into the process that the fraudulent account still held $11,000, which the large bank had withheld from us. It took three requests before they returned even that amount, over a year after the incident.

A more effective interbank dispute resolution process would enable community banks to pursue check fraud claims much more efficiently, increasing certainty across the ecosystem.

Question 3

Mrs. Dempsey, to the best of your knowledge, do large financial institutions face any penalties or consequences today when they deny legitimate fraud claims from community banks like yours?

Response:

I can best answer this question by describing our experience. In the case of our $118,000 cashier's check that was stolen and altered, we spent eight months simply trying to reach someone at the large depositing bank who could address our breach-of-warranty claim. We wrote letters, called every number we could find, and reached out to the Tennessee Bankers Association for help. When we finally identified someone who could supposedly help, he responded to our first email and then went silent when he learned what the issue concerned.

We hired a lawyer, at additional expense, and the claim was ultimately denied based on a determination that the check was "counterfeit" rather than "altered," even though the check number, amount, date, bank logo, address, signature, and other characteristics were all the same, and only the payee had been changed. We also learned ten months into the process that the fraudulent account still held $11,000, which the large bank had withheld from us. It took three requests before they returned even that amount, over a year after the incident. Our bank lost $118,000 plus legal fees.

More broadly, community banks report that large financial institutions often reject fraud claims even when we provide significant documentation. Contacts are difficult to find, and communication timeframes are often long. As a result, community banks are often forced to absorb losses when we have legitimate claims. The larger institution is not held to any timeliness standard and may not respond at all.

Question 4

Could a voluntary "senior fraud-protection account"—where older customers choose to put extra guardrails on their accounts, like tighter withdrawal limits and short delays on

large or out-of-pattern transactions—be one practical way banks could help stop these scams before a victim's entire savings is wiped out?

Response:

A voluntary senior fraud-protection account could help address a real problem that community banks see regularly. Community banks are uniquely positioned to prevent, detect, and mitigate fraud and scams, and we take this role very seriously.

In my testimony, I described an elderly woman without family in our community 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 our bank. Recognizing the likely scam, we refused her request to wire the money to the scammer and tried everything we could to convince her that it was a scam, including showing her FBI reports. But she didn't want to believe it. Romance scams are just that powerful. She then 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. She took the cash, went to a local convenience store with a Bitcoin ATM, deposited the money, and transferred it to the scammer. Today she lives in subsidized housing.

Had a voluntary senior fraud-protection account been in place, with features like tighter withdrawal limits and short delays on large or out-of-pattern transactions, it could have provided additional time for us to intervene. We recognized the scam immediately, but our ability to act was limited. Extra guardrails, voluntarily chosen by the customer, could give community bankers more ability to slow down suspicious transactions and protect vulnerable customers.

The data I cited in my testimony confirms the scale of this problem. The most recent IC3 report shows that people over 60 years of age reported, by a wide margin, the largest losses of any age group, at $4.8 billion in total. The FTC reports that the median loss is much higher among victims aged 70 to 79 ($1,000) and aged 80 and above ($1,650) compared to the overall median of $499.

As relationship bankers, community banks know their customers in real and meaningful ways. Our staff are the point of customer contact and positioned to detect fraud early and intervene. Their training is important, but so are the personal relationships they have formed with customers. Our team did everything they could in this case, but our ability to act was limited. A voluntary senior fraud-protection account could give us an additional tool to help prevent these losses.

Questions for the Record

Subcommittee on Financial Institutions Hearing

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

March 5, 2026

From Rep. Rose:

1. **Mr. McDade, we've heard far too many heartbreaking stories in Tennessee of seniors caught up in romance scams, emptying their accounts at the insistence of a scammer and never seeing that money again. It seems clear the status quo isn't protecting them. Could a voluntary "senior fraud-protection account"—where older customers choose to put extra guardrails on their accounts, like tighter withdrawal limits and short delays on large or out-of-pattern transactions—be one practical way banks could help stop these scams before a victim's entire savings is wiped out?**

Congressman, the stories are deeply troubling and underscore why CBA has called for a whole-of-government approach to combat scams affecting millions of Americans. Unlike fraud, which targets financial institutions directly, scams involve criminals deceiving consumers, often through phone, text, or online channels, into sending money themselves.

These scams typically occur outside the bank's control, with banks only becoming aware once a transaction is initiated. That's why prevention must focus on where the deception happens, and today, our most effective tool is expanding consumer awareness and protections across those external channels.

Scams are getting more sophisticated to trick consumers out of their own money. CBA members develop banking products that meet modern demand while offering enhanced fraud protections to security conscious consumers. In the age of the iPhone, customers increasingly want their banking services to feel as quick and simple as an Amazon order. Financial institutions, including members of CBA, must continually balance speed with safety to provide the best experience possible.

Regional banks, like EverBank provide numerous resources to help our customers combat scams including warnings and customer education. We also invest significant time and resources into specialized staff training, the integration of advanced fraud prevention technology, and the implementation of programs designed to identify and assist consumers who are at risk before they fall victim to schemes. We also focus on targeted customer training for fraud awareness,

collaborate with law enforcement agencies on specialized education, and utilize two-factor authentication and in-app messaging to keep our clients informed.

By taking proactive steps, including monitoring unusual account activity, educating customers about common and emerging fraud and scam techniques, and creating policies that prioritize customer protection, banks support the main street communities and protect the customers they serve. Ultimately, these efforts reinforce trust, strengthen long-term customer relationships, and help create a safer financial environment for everyone across the banking ecosystem.

The discussion draft legislation, noticed for the hearing, titled the Scrutinizing Transactions for Overt Payment Fraud Act, or the STOP Fraud Act, represents another vital tool for banks.[1] By amending the Expedited Funds Availability Act, this legislation would allow financial institutions to delay the availability of funds when they have reasonable cause to suspect fraud. The ability to review suspicious transactions when there is reasonable cause to believe a malicious actor is involved would benefit senior citizens, as well as all customers who might be victims of a scam

Yet, generally these scams originate, or are otherwise facilitated, outside of the banking system, through social media, telephone and texts messages, and crypto platforms. This means that Bank's don't know about the scam until a customer's request to move money. While banks try to warn customers that they may be falling victim to a scam, there are instances where customers may not adhere to these warnings. Importantly, it is the role of banks to send money where the customer directs, often on timelines required by regulations. It is not just a matter of stopping the customer from sending the money, it is a matter of targeting the origination of these scams on social media platforms and text messages, of preventing the spoofing of phone numbers that are used to further deceive customers, of ensuring there is adequate prosecution of these scammers to deter further scam activity. It is also important for government and relevant industries alike to facilitate effective education for consumers of all ages that informs them of the warning signs of, and what to do when they encounter these sophisticated scams, which is why we support a national campaign for scam awareness, similar to the United Kingdom.

---

[1] H.R., 119th Cong., *Scrutinizing Transactions for Overt Payment Fraud Act of 2026*, (last visited Apr. 6, 2026), *available here*.

Subcommittee on Financial Institutions Hearing
"Fighting Fraud on the Front Lines: Challenges and Opportunities for Financial Institutions" Questions for the Record
March 5, 2026

Answer From Ms. Kate McKune, General Counsel, Park Community Credit Union, Louisville, KY, on behalf of America's Credit Unions, to Question from Rep. Rose:

1. Ms. McKune, we've heard far too many heartbreaking stories in Tennessee of seniors caught up in romance scams, emptying their accounts at the insistence of a scammer and never seeing that money again. It seems clear the status quo isn't protecting them. Could a voluntary "senior fraud-protection account"—where older customers choose to put extra guardrails on their accounts, like tighter withdrawal limits and short delays on large or out-of-pattern transactions—be one practical way banks could help stop these scams before a victim's entire savings is wiped out?

   Yes, a voluntary "senior fraud-protection account" or voluntary trusted contact account (because there are vulnerable individuals beyond just seniors) can be a way to help combat scams if done well. I would note that it is important that such tools should not create heavy burdens or liability on the financial institutions that try to help. How an individual opts into or out of a "senior fraud protection account" should involve a process that is itself resistant to fraud.

Ballard Spahr LLP

1800 Larimer Street, Suite 1600
Denver, CO 80202-1408
tel 303.292.2400
fax 303.296.3956
www.ballardspahr.com

Joseph Schuster
Tel: 303.299.7327
Fax: 303.296.3956
schusterj@ballardspahr.com

April 10, 2026

The Honorable French Hill
Chairman
Committee on Financial Services
United States House of Representatives
2129 Rayburn House Office Building
Washington, DC 20515

Re: Responses to Questions for the Record Submitted by Representative Rose

Dear Chairman Hill:

Thank you for the opportunity to provide responses to the Questions for the Record submitted following the March 5, 2026 hearing entitled "Fighting Fraud on the Front Lines: Challenges and Opportunities for Financial Institutions."

Set forth below are my responses to the questions submitted by Representative Rose.

From Representative Rose:

1. Mr. Schuster, your testimony highlights document fraud and digital identity manipulation. One area where this is becoming a major issue is the impact of fraud in rental housing. We're seeing a sharp rise in fake pay stubs, bogus bank statements, and fabricated IDs being used on rental applications, and when those tenants inevitably default, it can also harm financial institutions that have made loans on those rental properties based on what turned out to be fraudulent documentation. What steps can housing providers take to better detect and prevent fraudulent documents in the rental application process?

2. Mr. Schuster, we've heard far too many heartbreaking stories in Tennessee of seniors caught up in romance scams, emptying their accounts at the insistence of a scammer and never seeing that money again. It seems clear the status quo isn't protecting them. Could a voluntary "senior fraud-protection account"—where older customers choose to put extra guardrails on their

accounts, like tighter withdrawal limits and short delays on large or out-of-pattern transactions—be one practical way banks could help stop these scams before a victim's entire savings is wiped out?

Response to Question 1:

Thank you, Representative Rose. You are exactly right to highlight rental housing as an emerging pressure point for document fraud, and it reflects a broader theme from my testimony: fraud today is coordinated and network-based, while detection often remains fragmented across institutions and, in many cases, still reliant on manual review of static documents, even as fraudsters leverage increasingly sophisticated, technology-enabled tools.

Housing providers should, where possible, take steps at the point of application to reduce reliance on static, applicant-provided documents. This can include moving toward source-based verification, such as confirming income or account information directly with payroll providers or financial institutions, and implementing layered identity checks that evaluate consistency across the application, supporting information, and other available data sources. Controls such as standardized verification procedures, direct employer or financial institution confirmation, and escalation of higher-risk applications can meaningfully improve detection. These measures help shift the process away from documents that are increasingly easy to fabricate and toward more reliable, verifiable data.

However, the most effective long-term solution requires expanding the fraud information-sharing ecosystem beyond traditional financial institutions and making it accessible, in an appropriate and controlled manner, to housing providers and similar market participants.

Today, financial institutions often have visibility into fraud signals that would be highly relevant to rental screening, including indicators associated with mule accounts, synthetic identities, or patterns of document manipulation. At the same time, housing providers may be encountering the front end of those same schemes through fraudulent applications. However, there is no clear, real-time, and legally streamlined framework that allows those signals to be shared across that broader ecosystem.

Existing mechanisms, such as information sharing under Section 314(b) of the USA PATRIOT Act, are helpful, but they are primarily designed around anti-money laundering objectives and generally do not extend in a practical way to housing providers or to modern document fraud typologies. As a result, we have a structural mismatch. Individual actors can now use widely available tools to create convincing fake documents, while defenders such as banks, landlords, and property managers remain siloed and often lack the resources to respond effectively.

There is a meaningful opportunity for policymakers to address this by:

1. Clarifying and expanding safe harbors for fraud-related information sharing, including under frameworks such as the Fair Credit Reporting Act, so that financial institutions can

share targeted fraud indicators without concern that doing so creates unintended regulatory obligations;

2. Modernizing and potentially extending information-sharing frameworks, such as Section 314(b), to expressly cover coordinated fraud prevention and to allow participation by appropriately scoped non-bank actors, including housing providers or their service platforms; and

3. Encouraging standardized, privacy-protective fraud signal exchanges, where limited, high-value indicators such as identity inconsistencies or known fraudulent document patterns can be shared in real time.

Importantly, this can be accomplished in a manner that preserves consumer protections and privacy by limiting the scope of data shared, requiring good-faith use for fraud prevention, and incorporating appropriate governance and oversight.

In short, while housing providers can strengthen their own front-end controls, the larger opportunity is to connect them into the same coordinated fraud defense frameworks that financial institutions are building. That kind of cross-sector visibility is increasingly necessary to address fraud that is, by its nature, cross-platform and highly coordinated.

Response to Question 2:

The stories you are describing are deeply concerning, and they reflect one of the most difficult challenges in modern fraud prevention. In many of these cases, the transaction is technically authorized, but it is the product of deception and manipulation. That makes intervention both more important and more complex.

The concept you describe, a voluntary "senior fraud-protection account" with additional guardrails, is a constructive and practical approach. Providing customers, particularly older consumers, with the option to opt into enhanced protections such as transaction delays, lower thresholds for review, or trusted contact notifications can be an effective way to introduce friction where it is most needed, while preserving autonomy and access.

At the same time, it is important to recognize the practical realities. Many consumers, including seniors, rely on timely access to their funds for legitimate and sometimes urgent needs. Overly rigid controls or delays applied across the board can create real hardship and may discourage use of the very protections designed to help them. That is why flexibility and consumer choice are critical. These types of tools are most effective when they are risk-based, customizable, and supported by clear communication so that customers understand both the protections and the tradeoffs.

More broadly, as I noted in my testimony, point-of-transaction controls, while important, are only one part of the solution. Fraud today is fast-moving, cross-platform, and often involves

multiple institutions and payment channels. Individual institutions frequently see only a portion of the overall scheme.

That is why a more holistic approach is necessary. This includes:

1. Expanding information sharing so institutions can identify scam patterns and mule accounts earlier;

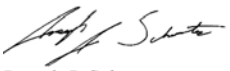
2. Enabling real-time, cross-institution coordination to interrupt suspicious transfers before funds are dissipated; and

3. Providing clearer legal frameworks and safe harbors so institutions can apply targeted, risk-based interventions without hesitation.

Voluntary account-level protections can play an important role within that broader framework. When combined with improved information sharing, better real-time detection, and clear legal support for proactive intervention, tools that empower consumers to opt into additional safeguards can help create a layered defense that is much more effective against these types of scams.

Thank you for the opportunity to provide these responses. Please do not hesitate to contact me if additional information would be helpful.

Sincerely,



Joseph J. Schuster
Partner, Ballard Spahr LLP

Question 1

From the perspective of community banks and credit unions, how helpful would expanded law enforcement capabilities around blockchain tracing be in combating cryptocurrency-related scams, and how can financial institutions better coordinate with law enforcement when these digital asset transactions intersect with the traditional banking system?

Response:

While my testimony focused primarily on check fraud and imposter scams, I can speak to how cryptocurrency intersects with the fraud we see at the community bank level.

As I described in my testimony, an elderly customer of ours who fell victim to a romance scam ultimately withdrew her money in cash and transferred it to the scammer through a Bitcoin ATM at a local convenience store. Despite our best efforts to intervene, the funds were gone and the scammer was never heard from again.

On the question of coordination with law enforcement, in one case our bank worked with a victim and the local sheriff to create a sting operation that led to the arrest of a fraudster. I am proud of the role our bank played in that case. As I stated in my testimony, the problem of fraud is urgent and must be fought through coordination among financial institutions of all charter types and sizes, law enforcement, and government at every level.

Subcommittee on Financial Institutions Hearing
"Fighting Fraud on the Front Lines: Challenges and Opportunities for Financial Institutions" Questions for the Record
March 5, 2026

Answers From Ms. Kate McKune, General Counsel, Park Community Credit Union, Louisville, KY, on behalf of America's Credit Unions, to Question from Rep. Fitzgerald:

Remarks: "Financial fraud is hitting Americans harder than ever. Wisconsin consumers and businesses have lost more than $107 million to fraud to date, including $32.8 million in the third quarter of 2025 alone. These crimes increasingly rely on fast-moving digital networks that local law enforcement simply isn't equipped to trace on its own. That's why I'm proud to cosponsor the ***GUARD Act*** *alongside Representatives Nunn and Gottheimer. This bill would give State, local, and Tribal law enforcement the ability to use existing federal grants to purchase blockchain-tracing software and training investigators on emerging technology. It also* ***clarifies that Federal law enforcement can assist local agencies with blockchain tracing tools****, closing a major coordination gap that criminals have been exploiting."*

1. From the perspective of community banks and credit unions, how helpful would expanded law enforcement capabilities around blockchain tracing be in combating cryptocurrency-related scams, and how can financial institutions better coordinate with law enforcement when these digital asset transactions intersect with the traditional banking system?

From a credit union's perspective, this sounds like it would be very helpful. One of the challenges financial institutions often face is that law enforcement does not have the time/tools/resources to help combat financial fraud when they are often dealing with other crimes. Giving law enforcement new tools to work and coordinate with financial institutions would be a good thing. If these tools (or the information generated by them) can be shared with financial institutions, it would potentially ease BSA/AML compliance burdens associated with nascent business models focused on stablecoins or other digital assets.

2. Credit unions consistently emphasize the impact that fraud has not only on the institutions themselves but also on their members. Can you speak to the tangible costs that fraud imposes on consumers, including credit union members, and how strengthened fraud prevention efforts ultimately reduce those costs. Additionally, what kinds of resources or operational capacity would credit unions be able to free up if the burden of fraud were reduced, and how would those savings translate into improved service or lower costs for members?

At Park Community our fraud prevention efforts helped stop over $1 million in fraud in 2025, but our charge-offs from fraud were still over $300,000 in both 2024 and 2025. Additionally, we issued nearly 6,500 fraud alerts in 2025. We spend a lot of resources and time on staff training to combat fraud. As a not-for-profit cooperative, the dollars we spend to fight fraud come from the money we could otherwise use to help our members in other ways, from making more loans to providing better rates. If the burden of fraud were reduced, we would be able to reallocate funds used to cover fraud-related expenses in ways that directly help our members.

We are also very cognizant of the impact of fraud at the individual member level. While we take many steps as an institution to educate and help our members, fraudsters often appeal to the frailties of human nature, and there is only so much we can do. We've seen romance scammers spend years cultivating a member before seeking funds from them. Online scams for fake or misleading goods can target consumers. While fraudsters deceiving a consumer out of hundreds of dollars may not warrant the close engagement of law enforcement, for that consumer it can be a life-altering event that can impact their ability to pay bills or even to eat. A comprehensive national strategy to combat fraud and educate consumers as I outlined in my written testimony would go a long way to helping consumers.

Ballard Spahr LLP

1800 Larimer Street, Suite 1600
Denver, CO 80202-1408
tel 303.292.2400
fax 303.296.3956
www.ballardspahr.com

Joseph Schuster
Tel: 303.299.7327
Fax: 303.296.3956
schusterj@ballardspahr.com

April 10, 2026

The Honorable French Hill
Chairman
Committee on Financial Services
United States House of Representatives
2129 Rayburn House Office Building
Washington, DC 20515

Re: Response to Question for the Record Submitted by Representative Fitzgerald

Dear Chairman Hill:

Thank you for the opportunity to provide responses to the Questions for the Record submitted following the March 5, 2026 hearing entitled "Fighting Fraud on the Front Lines: Challenges and Opportunities for Financial Institutions."

Set forth below is my response to the question submitted by Representative Fitzgerald.

From Representative Fitzgerald:

*Remarks: "Financial fraud is hitting Americans harder than ever. Wisconsin consumers and businesses have lost more than $107 million to fraud to date, including $32.8 million in the third quarter of 2025 alone. These crimes increasingly rely on fast-moving digital networks that local law enforcement simply isn't equipped to trace on its own. That's why I'm proud to cosponsor the **GUARD Act** alongside Representatives Nunn and Gottheimer. This bill would give State, local, and Tribal law enforcement the ability to use existing federal grants to purchase blockchain-tracing software and training investigators on emerging technology. It also **clarifies that Federal law enforcement can assist local agencies with blockchain tracing tools**, closing a major coordination gap that criminals have been exploiting."*

1. On February 23rd, the FTC and DOJ announced they were seeking to revise their Antitrust Guidelines for Business Collaborations, which have not been updated since the year 2000. There has been some concern amongst banks and financial firms that certain business collaboration for the purposes of fraud detection and mitigation could be subject to antitrust scrutiny under the

Sherman Act. Is that the type of collaboration you hope FTC and DOJ will clarify in updating their guidelines, or do financial institutions need more clarification from Congress?

Response:

Updated guidance from the Department of Justice and Federal Trade Commission would be helpful, particularly if it makes clear that appropriately scoped information sharing for fraud detection and prevention is a pro-competitive activity. However, many financial institutions are likely to remain cautious absent clearer statutory protection. For that reason, a targeted Congressional safe harbor for fraud-prevention collaboration would be highly beneficial. A framework modeled on existing regimes, such as cybersecurity information sharing and anti-money laundering information sharing under Section 314(b) of the USA PATRIOT Act, could provide the certainty institutions need to collaborate effectively while maintaining appropriate safeguards. Such a safe harbor could be appropriately limited to good-faith information sharing for fraud detection and prevention, subject to reasonable guardrails addressing data use, confidentiality, and consumer protection.

Fraud today is highly networked and often spans multiple institutions and multiple payment rails, including blockchain networks. Individual institutions frequently see only fragments of a broader scheme. The ability to share indicators, typologies, and blockchain-related intelligence in a timely manner could materially reduce consumer harm and improve the effectiveness of both private-sector and law enforcement responses.

At the same time, developments in blockchain technology present a meaningful opportunity to enhance fraud detection and recovery. Many blockchain transactions occur on public, transparent ledgers, which can allow investigators to trace the movement of funds across wallets and over time in ways that are not always possible with cash or certain legacy payment systems. With appropriate analytic tools and responsible information sharing, this visibility can support earlier identification of fraud networks, more efficient investigations, and, where appropriate, the freezing or recovery of funds. In this respect, blockchain technology can serve as a valuable tool for law enforcement and financial institutions in detecting, investigating, and mitigating fraud, not solely as a payment mechanism.

Congress can play an important role by establishing clear legal frameworks that encourage responsible collaboration and the use of emerging technologies for fraud prevention, while maintaining appropriate privacy and competition safeguards. If structured carefully, such a framework could help ensure that fraud is identified earlier, losses are reduced, and both consumers and financial institutions are better protected.

Thank you for the opportunity to provide this response. Please do not hesitate to contact me if additional information would be helpful.

Sincerely,



Joseph J. Schuster
Partner, Ballard Spahr LLP

[DISCUSSION DRAFT]

119TH CONGRESS
2D SESSION

H. R. _____

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

IN THE HOUSE OF REPRESENTATIVES

M__. _____ introduced the following bill; which was referred to the Committee on _____

A BILL

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

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Transaction Risk Analytics and Collaborative Exchange Act of 2026" or the "TRACE Act of 2026".

SEC. 2. DEFINITIONS.

In this Act:

(1) ARTIFICIAL INTELLIGENCE SYSTEM.—The term ''artificial intelligence system'' means any machine-learning, neural-network, statistical, or automated pattern-recognition system used to analyze covered information for a covered fraud-prevention purpose.

(2) COVERED FRAUD-PREVENTION PURPOSE.—The term ''covered fraud-prevention purpose'' means the detection, prevention, mitigation, or investigation of fraud, scams, identity theft, account takeover, synthetic identity fraud, money-mule activity, or cyber-enabled theft.

(3) COVERED INFORMATION.—The term ''covered information'' means transactional indicators, device or network identifiers, tokenized or hashed personal identifiers, behavioral patterns, typologies, risk signals, and similar data reasonably necessary to carry out a covered fraud-prevention purpose.

(4) FEDERAL FINANCIAL REGULATOR.—The term ''Federal financial regulator'' means—

(A) a Federal banking agency, as defined in section 3 of the Federal Deposit Insurance Act (12 U.S.C. 1813); and

(B) the National Credit Union Administration.

(5) FINANCIAL INSTITUTION.—The term ''financial institution'' has the meaning given that term in section 603(t) of the Fair Credit Reporting Act (15 U.S.C. 1681a(t)).

SEC. 3. AUTHORIZATION FOR FRAUD INFORMATION SHARING AND CONFORMING AMENDMENTS.

(a) AMENDMENT TO THE GRAMM-LEACH-BLILEY ACT.—Section 502 of the Gramm-Leach-Bliley Act (15 U.S.C. 6802) is amended by adding at the end the following:

''(f) FRAUD-PREVENTION INFORMATION SHARING.—

''(1) IN GENERAL.—Notwithstanding subsections (a) through (e), a financial institution may disclose nonpublic personal information to a financial institution or to a fraud-information-sharing system, solely for a covered fraud-prevention purpose.

''(2) PERMITTED USES.—Information disclosed under paragraph (1) may be used for—

''(A) real-time or batch fraud monitoring;

''(B) training, testing, or validating artificial intelligence systems;

''(C) generation of typologies, indicators, or risk signals; and

"(D) other uses approved by regulation that are consistent with a covered fraud-prevention purpose.

"(3) CONDITIONS.—Nonpublic personal information disclosed pursuant to paragraph (1) shall be subject to the requirements of this title otherwise applicable to disclosed nonpublic personal information.

"(4) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to permit the use of nonpublic personal information for marketing, underwriting, pricing, or credit eligibility determinations, except as otherwise permitted by law.

"(5) DEFINITIONS.—In this subsection, the terms 'artificial intelligence system', 'financial institution', and 'covered fraud-prevention purpose' have the meaning given those terms, respectively, in section 2 of the TRACE Act of 2026.".

(b) AMENDMENTS TO THE FAIR CREDIT REPORTING ACT.—The Fair Credit Reporting Act (15 U.S.C. 1681 et seq.) is amended—

(1) by inserting after section 623 the following:

"SEC. 623A. FRAUD-PREVENTION INFORMATION-SHARING SYSTEMS.

"(a) IN GENERAL.—A fraud-information-sharing system operated solely for covered fraud-prevention purposes shall not be treated as a consumer reporting agency for purposes of this title.

"(b) LIMITATIONS.—Subsection (a) shall apply only if—

"(1) information is not used for marketing, underwriting, or pricing;

"(2) reasonable procedures are maintained to assure accuracy; and

"(3) consumers retain any rights otherwise provided under this title when an adverse action is based solely on information obtained through such a system.

"(c) COVERED FRAUD-PREVENTION PURPOSE DEFINED.—In this section, the term 'covered fraud-prevention purpose' has the meaning given that term in section 2 of the TRACE Act of 2026."; and

(2) in the table of contents for such Act, by inserting after the item relating to section 623 the following:

"623A. Fraud-prevention information-sharing systems.".

(c) AMENDMENTS TO THE RIGHT TO FINANCIAL PRIVACY ACT OF 1978.—Section 1113 of the Right to Finan-

cial Privacy Act of 1978 (12 U.S.C. 3413) is amended by adding at the end the following:

"(s) FRAUD-PREVENTION INFORMATION SHARING.—

"(1) IN GENERAL.—Nothing in this chapter shall prohibit a financial institution from transmitting covered information to Federal regulators or law-enforcement agencies through a fraud-information-sharing system, solely for a covered fraud-prevention purpose.

"(2) DEFINITIONS.—The terms 'covered fraud-prevention purpose' and 'covered information' have the meaning given those terms, respectively, in section 2 of the TRACE Act of 2026.".

[DISCUSSION DRAFT]

119TH CONGRESS
2D SESSION

H. R. _____

To 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, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

M__. _____ introduced the following bill; which was referred to the Committee on _____

A BILL

To 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, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Bank Fraud Technology Advancement Act of 2026".

SEC. 2. DEFINITIONS.

In this Act:

(1) ADVANCED FRAUD DETECTION TECHNOLOGY.—The term ''advanced fraud detection technology'' includes artificial intelligence, machine learning, predictive analytics, behavioral biometrics, network analytics, data fusion tools, distributed ledger-based monitoring tools, blockchain tracing tools, and other emerging technologies used to detect, prevent, or mitigate financial fraud.

(2) ARTIFICIAL INTELLIGENCE.—The term ''artificial intelligence'' has the meaning given that term in section 5002 of the National Artificial Intelligence Initiative Act of 2020 (15 U.S.C. 9401).

(3) COMMUNITY FINANCIAL INSTITUTION.—The term ''community financial institution'' means—

(A) an insured depository institution with total consolidated assets of $10,000,000,000 or less; and

(B) a credit union with total assets of $10,000,000,000 or less.

(4) CREDIT UNION.—The term ''credit union'' means a State credit union or Federal credit union, as such terms are defined, respectively, in section 101 of the Federal Credit Union Act (12 U.S.C. 1752).

(5) FEDERAL BANKING AGENCY.—The term ''Federal banking agency''—

(A) has the meaning given such term in section 3 of the Federal Deposit Insurance Act (12 U.S.C. 1813); and

(B) means the National Credit Union Administration.

(6) INSURED DEPOSITORY INSTITUTION.—The term ''insured depository institution'' has the meaning given such term in section 3 of the Federal Deposit Insurance Act (12 U.S.C. 1813).

(7) MACHINE LEARNING.—The term ''machine learning'' has the meaning given that term in section 5002 of the National Artificial Intelligence Initiative Act of 2020 (15 U.S.C. 9401).

SEC. 3. STUDY ON ADVANCED TECHNOLOGIES IN FRAUD DETECTION AND PREVENTION.

(a) IN GENERAL.—The Federal banking agencies, in consultation with the Secretary of the Treasury, the Financial Crimes Enforcement Network, the Federal Trade Commission, and appropriate law enforcement agencies, shall jointly conduct a comprehensive study on the use of advanced fraud detection technology by insured depository institutions and credit unions.

(b) REQUIRED ELEMENTS.—The study required under subsection (a) shall evaluate the following:

(1) CURRENT USE AND EFFECTIVENESS.—The current use and effectiveness of advanced fraud detection technology, including—

(A) the extent to which insured depository institutions and credit unions of varying asset sizes deploy advanced fraud detection technology;

(B) measurable outcomes relating to fraud reduction, loss mitigation, and consumer protection; and

(C) barriers to adoption, including cost, vendor concentration, interoperability constraints, regulatory uncertainty, data access limitations, and liability concerns.

(2) COMMUNITY FINANCIAL INSTITUTION ACCESS.—Community financial institution access to advanced fraud detection technology, including—

(A) challenges faced by community financial institutions in accessing or deploying advanced fraud detection tools;

(B) whether economies of scale disadvantage smaller community financial institutions

relative to large community financial institutions;

(C) options to facilitate shared services, utility models, managed-service providers, or consortium-based fraud detection platforms; and

(D) recommendations to ensure regulatory guidance is appropriately tailored to avoid discouraging adoption by smaller community financial institutions.

(3) ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING.—Artificial intelligence and machine learning, including—

(A) the use of artificial intelligence and machine learning models, applications, and tools in detecting fraud patterns, anomalies, synthetic identity fraud, and real-time payment fraud;

(B) governance frameworks used by insured depository institutions and credit unions to manage fraud model risk, explainability, bias, and validation; and

(C) interactions between fraud detection models and consumer protection laws, including

fair lending and unfair, deceptive, or abusive acts or practices standards.

(4) INFORMATION SHARING AND PUBLIC-PRIVATE PARTNERSHIPS.—Information sharing and public-private partnerships, including—

(A) the effectiveness of existing information-sharing frameworks, including section 314(b) of the USA PATRIOT Act (31 U.S.C. 5311 note);

(B) whether expanded public-private partnerships or centralized fraud utilities would enhance detection capabilities;

(C) the feasibility of a voluntary fraud analytics consortium accessible to community financial institutions; and

(D) privacy, data protection, and cybersecurity considerations associated with expanded data sharing.

(5) PAYMENTS SYSTEM RISKS.—Payments system risk, including—

(A) fraud risks associated with instant payments, wire transfers, ACH transactions, check fraud, and emerging payment channels; and

(B) whether advanced analytics can reduce fraud while preserving settlement finality and payment system stability.

(6) REGULATORY AND SUPERVISORY CONSIDERATIONS.—Regulatory and supervisory considerations, including—

(A) whether existing supervisory expectations create unintended barriers to innovation;

(B) the need for interagency guidance, regulatory clarity, or safe harbors to support technology adoption; and

(C) opportunities to harmonize expectations across Federal banking agencies.

(c) REPORT AND RECOMMENDATIONS.—

(1) REPORT.—Not later than 18 months after the date of enactment of this Act, the Federal banking agencies shall issue a report to the Committee on Financial Services of the House of Representatives and the Committee on Banking, Housing, and Urban Affairs of the Senate containing all findings and determinations made in carrying out the study required under this section, and make such report publicly available, except for classified or supervisory information.

(2) RECOMMENDATIONS.—The report required under paragraph (1) shall include legislative, regulatory, or supervisory recommendations which may include—

(A) proposals to support shared fraud detection utilities or consortium-based analytics platforms;

(B) guidance or safe harbors to encourage responsible artificial intelligence use in fraud prevention;

(C) options to reduce vendor concentration risk;

(D) pilot programs or regulatory sandboxes tailored to community financial institutions; and

(E) recommendations to strengthen public-private information sharing consistent with privacy and civil liberties protections.

SEC. 4. COMMUNITY BANK FRAUD TECHNOLOGY PILOT PROGRAM.

(a) IN GENERAL.—Not later than 1 year after submission of the study under section 3, the Federal banking agencies may jointly establish a voluntary pilot program to facilitate community financial institution access to advanced fraud detection tools.

(b) PROGRAM FEATURES.—The pilot program described in subsection (a) may include—

(1) pooled procurement or shared services models;

(2) model validation assistance or technical support;

(3) standardized vendor risk management templates;

(4) regulatory clarity regarding model governance expectations; and

(5) collaboration with the Department of the Treasury and law enforcement to provide anonymized fraud typology data feeds.

[DISCUSSION DRAFT]

119TH CONGRESS
2D SESSION

H. R. _____

To amend the Expedited Funds Availability Act to provide exceptions in the case of fraudulent checks or wire transfers, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

M__. _____ introduced the following bill; which was referred to the Committee on _____

A BILL

To amend the Expedited Funds Availability Act to provide exceptions in the case of fraudulent checks or wire transfers, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Scrutinizing Transactions for Overt Payment Fraud Act of 2026" or the "STOP Fraud Act of 2026".

SEC. 2. EXCEPTION TO FUNDS AVAILABILITY REQUIREMENTS IN THE CASE OF TREASURY CHECK FRAUD OR CASHIER'S CHECK FRAUD.

Section 604(c)(1) of the Expedited Funds Availability Act (12 U.S.C. 4003(c)(1)) is amended to read as follows:

"(1) IN GENERAL.—

"(A) REGULATIONS.—In accordance with regulations which the Board shall prescribe, subsections (a)(2), (b), (c), and (e) of section 603 shall not apply with respect to—

"(i) any check deposited in an account at a depository institution if the receiving depository institution has reasonable cause to believe that the check is uncollectible from the originating depository institution;

"(ii) any cashier's check, certified check, teller's check, or depository check, or any check purporting to be a cashier's check, certified check, teller's check, or depository check, if the receiving depository institution has reasonable cause to believe that the check is forged or otherwise fraudulent; or

"(iii) any check drawn on, or purportedly drawn on, the Treasury of the United

States if the receiving depository institution has reasonable cause to believe that the check is forged or otherwise fraudulent.

"(B) REASONABLE CAUSE.—For purposes of this paragraph, reasonable cause to believe requires the existence of facts which would cause a well-grounded belief in the mind of a reasonable person. Such reasons shall be included in the notice required under subsection (f).".

SEC. 3. EXCEPTION TO FUNDS AVAILABILITY REQUIREMENTS IN THE CASE OF FRAUDULENT WIRE TRANSFERS.

Section 604 of the Expedited Funds Availability Act (12 U.S.C. 4003) is amended by adding at the end the following:

"(g) REASONABLE CAUSE EXCEPTION FOR WIRE TRANSFERS.—

"(1) IN GENERAL.—In accordance with regulations which the Board shall prescribe, section 603(a)(1)(B) shall not apply with respect to funds received by a depository institution by wire transfer if the receiving depository institution has reasonable cause to believe that the wire transfer was induced

fraudulently or is otherwise part of a scheme or artifice to defraud any person. For purposes of the preceding sentence, reasonable cause to believe requires the existence of facts which would cause a well-grounded belief in the mind of a reasonable person. Such reasons shall be included in the notice required under subsection (f).

"(2) BASIS FOR DETERMINATION.—No determination under this subsection may be based on any class of wire transfers or persons.

"(3) OVERDRAFT FEES.—If the receiving depository institution determines that a wire transfer for credit to an account is a wire transfer described in paragraph (1), the receiving depository institution shall not assess any fee for any subsequent overdraft with respect to such account, if—

"(A) the depositor was not provided with the written notice required under subsection (f) (with respect to such determination) at the time the wire transfer was delayed for credit; and

"(B) the overdraft would not have occurred but for the fact that the funds so transferred are not available.

"(4) COMPLIANCE.—Each agency referred to in section 610(a) shall monitor compliance with the re-

quirements of this subsection in each regular examination of a depository institution and shall describe in each report to the Congress the extent to which this subsection is being complied with. For the purpose of this paragraph, each depository institution shall retain a record of each notice provided under subsection (f) as a result of the application of this subsection.''.

SEC. 4. EXPEDITED FUNDS AVAILABILITY ACT RULEMAKING AUTHORITY.

The Expedited Funds Availability Act (12 U.S.C. 4001 et seq.) is amended—

(1) in section 603(d)(1) (12 U.S.C. 4002(d)(1)), by striking ''Board, jointly with the Director of the Bureau of Consumer Financial Protection,'' and inserting ''Board'';

(2) in section 604 (12 U.S.C. 4003)—

(A) by striking ''Board, jointly with the Director of the Bureau of Consumer Financial Protection,'' and inserting ''Board'' each place that term appears other than in subsection (f); and

(B) in subsection (f), by striking ''Board, jointly with the Director of the Bureau of Con-

sumer Financial Protection." and inserting "Board." each place that term appears;

(3) in section 605 (12 U.S.C. 4004)—

(A) by striking "Board, jointly with the Director of the Bureau of Consumer Financial Protection," and inserting "Board" each place that term appears; and

(B) in the heading of subsection (f)(1), by striking "BOARD AND BUREAU" and inserting "Board"; and

(4) in section 609 (12 U.S.C. 4008)—

(A) in subsection (a), by striking "Board, jointly with the Director of the Bureau of Consumer Financial Protection," and inserting "Board"; and

(B) by revising subsection (e) to read as follows:

"(e) CONSULTATIONS.—In prescribing regulations under subsections (a) and (b), the Board shall consult with the Comptroller of the Currency, the Board of Directors of the Federal Deposit Insurance Corporation, and the National Credit Union Administration Board.".

○