

FRAUD IN FOCUS: EXPOSING FINANCIAL THREATS TO AMERICAN FAMILIES

HEARING BEFORE THE SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS OF THE COMMITTEE ON FINANCIAL SERVICES U.S. HOUSE OF REPRESENTATIVES ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

SEPTEMBER 18, 2025

Serial No. 119–42

Printed for the use of the Committee on Financial Services



www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

63–431 PDF

WASHINGTON : 2026

HOUSE COMMITTEE ON FINANCIAL SERVICES

FRENCH HILL, Arkansas, *Chairman*

BILL HUIZENGA, Michigan, <i>Vice Chairman</i>	MAXINE WATERS, California, <i>Ranking Member</i>
FRANK D. LUCAS, Oklahoma	SYLVIA R. GARCIA, Texas, <i>Vice Ranking Member</i>
PETE SESSIONS, Texas	NYDIA M. VELÁZQUEZ, New York
ANN WAGNER, Missouri	BRAD SHERMAN, California
ANDY BARR, Kentucky	GREGORY W. MEEKS, New York
ROGER WILLIAMS, Texas	DAVID SCOTT, Georgia
TOM EMMER, Minnesota	STEPHEN F. LYNCH, Massachusetts
BARRY LOUDERMILK, Georgia	AL GREEN, Texas
WARREN DAVIDSON, Ohio	EMANUEL CLEAVER, Missouri
JOHN W. ROSE, Tennessee	JAMES A. HIMES, Connecticut
BRYAN STEIL, Wisconsin	BILL FOSTER, Illinois
WILLIAM R. TIMMONS, IV, South Carolina	JOYCE BEATTY, Ohio
MARLIN STUTZMAN, Indiana	JUAN VARGAS, California
RALPH NORMAN, South Carolina	JOSH GOTTHEIMER, New Jersey
DANIEL MEUSER, Pennsylvania	VICENTE GONZALEZ, Texas
YOUNG KIM, California	SEAN CASTEN, Illinois
BYRON DONALDS, Florida	AYANNA PRESSLEY, Massachusetts
ANDREW R. GARBARINO, New York	RASHIDA TLAIB, Michigan
SCOTT FITZGERALD, Wisconsin	RITCHIE TORRES, New York
MIKE FLOOD, Nebraska	NIKEMA WILLIAMS, Georgia
MICHAEL LAWLER, New York	BRITTANY PETTERSEN, Colorado
MONICA DE LA CRUZ, Texas	CLEO FIELDS, Louisiana
ANDREW OGLES, Tennessee	JANELLE BYNUM, Oregon
ZACHARY NUNN, Iowa	SAM LICCARDO, California
LISA McCLAIN, Michigan	
MARIA SALAZAR, Florida	
TROY DOWNING, Montana	
MIKE HARIDOPOLOS, Florida	
TIM MOORE, North Carolina	

Ben Johnson, *Staff Director*

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

DANIEL MEUSER, Pennsylvania, *Chairman*

TIM MOORE, North Carolina, <i>Vice Chairman</i>	AL GREEN, Texas, <i>Ranking Member</i>
ANN WAGNER, Missouri	RASHIDA TLAIB, Michigan
BARRY LOUDERMILK, Georgia	NIKEMA WILLIAMS, Georgia
ANDREW R. GARBARINO, New York	CLEO FIELDS, Louisiana
ANDREW OGLES, Tennessee	SAM LICCARDO, California
MIKE HARIDOPOLOS, Florida	

C O N T E N T S

Thursday, September 18, 2025

OPENING STATMENTS

	Page
Hon. Dan Meuser, Chairman of the Subcommittee on Oversight and Investigations, a U.S. Representative from Pennsylvania	2
Hon. Al Green, Ranking Member of the Subcommittee on Oversight and Investigations, a U.S. Representative from Texas	3

STATEMENTS

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

WITNESSES

Mr. Paul Benda, Executive Vice President of Risk, Fraud, and Cybersecurity, American Bankers Association (ABA)	5
Prepared Statement	8
Mr. Ian Bednowitz, General Manager, Lifelock at Gen	28
Prepared Statement	30
Ms. Kate Griffin, Director, National Task Force on Fraud and Scam Prevention, Aspen Institute Financial Security Program	38
Prepared Statement	40
Ms. Carla Sanchez-Adams, Senior Attorney, National Consumer Law Center (NCLC)	53
Prepared Statement	55

APPENDIX

MATERIALS SUBMITTED FOR THE RECORD

Hon. Dan Meuser:	
Consumer Bankers Association (CBA)	141
Bank Policy Institute (BPI)	143
AARP	165
American Financial Services Association (AFSA)	177
Securities Industry and Financial Markets Association (SIFMA)	179
Hon. Zachary Nunn, Hon. Hon. Josh Gottheimer, Hon. Scott Fitzgerald:	
Capital One	182

RESPONSES TO QUESTIONS FOR THE RECORD

Written responses to questions for the record from Representative Nikema Williams	
Mr. Paul Benda	185
Mr. Ian Bednowitz	
Ms. Kate Griffin	188
Ms. Carla Sanchez-Adams	190
Written responses to questions for the record from Representative Andrew R. Garbarino	
Ms. Kate Griffin	192

FRAUD IN FOCUS: EXPOSING FINANCIAL THREATS TO AMERICAN FAMILIES

Thursday, September 18, 2025

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,
COMMITTEE ON FINANCIAL SERVICES,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:02 a.m., in room 2128, Rayburn House Office Building, Hon. Dan Meuser [chairman of the subcommittee] presiding.

Present: Representatives Meuser, Wagner, Loudermilk, Ogles, Haridopolos, Moore, Green, Tlaib, Williams of Georgia, Fields, and Liccardo.

Also present: Representatives Hill, Lucas, Davidson, Steil, Nunn, Waters, and Foster.

Chairman MEUSER. Well, good morning, all.

The Subcommittee on Oversight and Investigations will come to order.

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

This hearing is entitled “Fraud in Focus: Exposing Financial Threats to American Families.” The purpose of this hearing is to better understand the various types of financial fraud that exist, including the meteoric rise in check fraud and senior scams.

This hearing will highlight different types of fraud and begin to identify opportunities for Federal agencies, both independently and together, and in conjunction and cooperatively with the private sector so we better use existing authorities to combat the rise in financial fraud and engage in consumer education.

This hearing will be the first in a series of fraud-and scam-related committee work. It is that important.

Without objection, all members will have 5 legislative days within which to submit extraneous materials to the chair for inclusion in the record.

Chairman MEUSER. I now recognize myself for 4 minutes to give an opening statement.

OPENING STATEMENT OF HON. DAN MEUSER, CHAIRMAN OF THE SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS, A U.S. REPRESENTATIVE FROM PENNSYLVANIA

I would like to thank the witnesses for being here today to discuss the fraud and scams in the financial sector and the threat they pose to consumers.

In 2024, the Federal Trade Commission (FTC) reported receiving 2.6 million reports of fraud and scams, with consumers losing over \$12 billion, a 25-percent increase from just 2023.

While that figure alone is staggering, it is likely only the tip of the iceberg, given that many victims do not report their experiences. In fact, the Department of Justice estimates that only 15 percent of victims report fraud to law enforcement.

Check fraud alone has more than doubled since 2021.

Criminals behind fraud and scams are sophisticated. They use a wide variety of schemes—check fraud, romance scams, bank transfer fraud, identity theft, payment scams, and more—and they target all segments of the population. Individuals of all ages are falling victim.

The only way to defeat criminals and defend consumers is truly a whole-society approach. Young adults are vulnerable, with so much of their personal information readily available online. Seniors, meanwhile, are often hit with the most devastating financial losses when exploited by scammers. All ages are at risk.

That is why today's hearing is not only about exposing the problem but also about discussing how we can best strengthen consumer education, highlight best practices for both consumers and companies, promote proven systems and models, and improve how we track and stop scammers before they strike.

I commend the Trump Administration for initiating efforts to counter fraud and scams in the U.S., including its recent sanctions on cyber scam centers based in Southeast Asia. President Trump also signed an executive order to move away from using checks for government-related payments.

The Treasury Department, the Federal Reserve, and the Securities and Exchange Commission have all recently initiated efforts to gain information pertaining to check fraud, payment fraud, and cross-border fraud.

To aid this effort, I sent a letter, along with Chairman Hill and Andy Barr, yesterday to Federal Reserve Chairman Jerome Powell seeking more information as to the Federal Reserve's (Fed's) work on fraud, including how it is collaborating with the Office of the Comptroller of the Currency (OCC), FDIC, and other stakeholders to address check and payment fraud.

We also requested a briefing on the comments received to the Fed's June 2025 request for information as well as the Fed's plans to educate consumers moving forward but no single actor can stop fraud on their own. To truly protect families, we must foster collaboration across all stakeholders. That includes working across Federal, State, and local governments, within the financial sector, including lending/payment companies and fraud protection companies, technology platforms, and telecom companies.

We are already seeing companies step up. Apple's recent iOS 26 update, for instance, expanded spam text and call screening to help consumers block fraud at the source.

Much more needs to be done, however. Conversations with all these stakeholders, including with consumers themselves, will be critical as we pursue a whole-of-society approach to combat fraud and scams.

Finally, I want to highlight that my office has just recently launched a new online resource at meuser.house.gov/scams, where consumers can learn red flags to spot scams, useful links to prevent fraud, and guidance on what to do if they fall victim.

So this is just the beginning of the committee's work and Congress's work on fraud and on scams. So I look forward to working on a bipartisan basis to find real solutions to a problem that continues to be the number one financial services issue I hear from my constituents, community banks, and law enforcement.

I yield back.

The chair now recognizes the ranking member of the subcommittee, the gentleman from Texas, Mr. Green, for 4 minutes for an opening statement.

OPENING STATEMENT OF HON. AL GREEN, RANKING MEMBER OF THE SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS, A U.S. REPRESENTATIVE FROM TEXAS

Mr. GREEN. I thank the chairman, someone whom I have great respect for, and I thank the witnesses for being here as well, as well as some other persons who are here at my request to show support. We greatly appreciate your attendance.

The title of this hearing is "Fraud in Focus: Exposing Financial Threats to American Families." However, a better title for this hearing would be "Fraud Enabled: How President Trump Is Exposing American Families to Financial Threats With His Tariff Taxes and His Evisceration of the Consumer Financial Protection Bureau," the CFPB.

When President Trump campaigned on imposing steep tariffs on both our allies and adversaries, he assured the American people that the cost of these tariffs would be paid by foreign sellers, not Americans.

This prevarication has become one of the biggest frauds in an administration rife with fraud. Instead of foreign sellers paying the price for Trump's tariffs, it is the buying U.S. businesses, in tandem with their clienteles, who are suffering the cost that foreign sellers will not pay.

Among the U.S. businesses suffering, small businesses have been especially vulnerable to the volatility of Trump's erratic economic policies. In July 2025, 67 percent of small businesses reported higher expenses over the quarter prior to that time. With 60 percent attributing higher costs to Trump's recent tariff increases, millions of mom-and-pop businesses are closing or are facing the prospect of closing.

Republicans desiring to combat fraud or financial threats to American families should focus on Trump's tariffs that are devastating American businesses, especially small businesses, as well as how Trump has systematically gutted the principal financial protection agency, the CFPB, and how the Consumer Financial Protection Bureau is being made ineffective.

The CFPB was established after the Great Recession to protect consumers from financial abuse, including fraud. Since its creation, the CFPB has actively protected consumers by investigating and punishing financial institutions for their abusive and deceptive practices. Since 2011, the CFPB has returned more than \$20 billion

to consumers defrauded by Big Banks, debt collectors, and payday lenders.

Sadly and shamefully, Trump's CFPB has stopped initiating new investigations into abuses in the financial industry and has discontinued ongoing examinations, dismissed enforcement actions, and even rescinded finalized settlements, denying consumers agreed-to benefits.

To add insult to consumer injuries, Republicans cut the CFPB's funding, cut it in half, crippling the agency's ability to police the payment processors Big Tech platforms and banks are using to take advantage of consumers.

The Republican record is clear: They have defrauded and dismantled the CFPB fraud police at the expense of the American consumers and have perpetrated a tax fraud on American families. Regrettably, this is not oversight; this is complicity, coupled with aiding and abetting Trump's fraud.

I yield back.

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

Chairman MEUSER. The gentleman yields back.

The chair now recognizes the chairman of the full committee, Chairman Hill, for 1 minute.

Chairman HILL. Thank you, Chairman Meuser.

Today's hearing is another step in the committee's efforts to better understand the various types of financial fraud so that we can better help protect American families from these financial threats.

Over the past 3 years, at one State bank trade association that I have gone to after another—Georgia, Mississippi, Arkansas, Louisiana, Texas, Ohio, among others—this has been the top topic.

Our State attorney generals are witnessing accelerated check fraud, debit fraud, and text phishing that are all targeting Americans and generating unprecedented losses to both consumers and the financial system. Personally, our family was a victim of check fraud, thanks to the U.S. post office, in 2022.

We will begin today by exploring a proactive set of measures that Federal agencies might take and implement to counter these threats and better protect all Americans from financial fraud.

We look forward to hearing about emerging technologies like AI and blockchain technologies that can help achieve that protection.

I thank our witnesses, and I yield back.

Chairman MEUSER. I thank Chairman Hill.

We will now move to witness testimony, seeing that the ranking member of the full committee is not here.

I really appreciate—we all appreciate your attendance and your, what we expect to be expert testimony.

We will start off by welcoming Mr. Paul Benda. Mr. Benda is the executive vice president of risk, fraud, and cybersecurity at the American Bankers Association, where he leads the American Bankers Association's (ABA's) initiative on fraud, cybersecurity, physical security, and information security and chairs the ABA Fraud Coordination Group. Mr. Benda also serves as the chair of the International Banking Federation's Scams and Fraud Task Force. Mr.

Benda's career spanned both public and private sectors, having served as an Active Duty U.S. Air Force officer and as an official with both the Department of Defense and Department of Homeland Security. Mr. Benda received a bachelor's and master's degree in mechanical engineering from Purdue University.

Welcome and thank you.

Mr. Ian Bednowitz: Mr. Bednowitz is the general manager of LifeLock at Gen, a leading U.S. identity-theft protection service. Prior to joining LifeLock, Mr. Bednowitz was the global head of protections at eBay, where he was responsible for managing and improving programs to build customers' trust for transacting on eBay. Mr. Bednowitz graduated summa cum laude with a B.A. in economics from Cornell University and holds an MBA from the Kellogg School of Management.

Thank you very much, and welcome.

Ms. Kate Griffin: Ms. Griffin is the director of the Aspen Institute's Financial Security Program. She also serves as the director of the National Task Force on Fraud and Scam Prevention, where she leads a multisector collaborative effort aimed at creating a national strategy to prevent scammers from stealing wealth from everyday Americans. She holds a master's from American University and a bachelor's degree from Kenyon College.

So thank you very much.

Ms. Carla Sanchez-Adams, welcome.

Ms. Sanchez-Adams is a senior attorney at the National Consumer Law Center. She also serves as a board member for the National Association of Consumer Advocates and is a fellow with the American Bar Association. Prior to joining National Consumer Law Center (NCLC), Ms. Sanchez-Adams was a managing attorney with Texas RioGrande Legal Aid. Ms. Sanchez-Adams graduated with a bachelor's degree from NYU and received her Juris Doctor from the University of Texas.

So thank you very much as well.

So 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.

So, Mr. Benda, you are now recognized for 5 minutes for your oral remarks.

STATEMENT OF PAUL BENDA, EXECUTIVE VICE PRESIDENT OF RISK, FRAUD, AND CYBERSECURITY, AMERICAN BANKERS ASSOCIATION

Mr. BENDA. Thank you, Mr. Chairman.

Chairman Meuser, Ranking Member Green, and members of the subcommittee, thank you for focusing on this critical issue today and the opportunity to testify.

My name is Paul Benda, and I serve as executive vice president of risk, fraud, and cybersecurity at the American Bankers Association.

Banks have long been on the front lines of protecting consumers from fraud. From chip-enabled cards to multifactor authentication, from AI-driven fraud detection to real-time alerts, the banking industry has invested billions to make our financial system one of the most secure in the world.

Americans recognize that effort. Surveys show that 9 in 10 customers say their bank is taking proactive steps to protect them from fraud, but criminals are innovating too. They have reinvested the \$300 billion stolen during the pandemic to build highly organized networks that now use deepfakes, spoofed caller IDs, stolen checks, and fake social media accounts to target Americans.

This is where banks face a critical limitation. By the time a victim is ready to send a payment, they often believe they know and trust the scammer. Caller ID might display the bank's name. A text message might look identical to a legitimate fraud alert. A social media ad might appear to come from a trusted company.

These are tools banks do not control. That is why banks cannot fight this battle alone. Other stakeholders must step up.

Telecommunication companies must stop criminals from impersonating banks through spoofed phone calls and fraudulent texts. Today, a criminal overseas can make a call appear as if it is coming from a 1-800 number on the back of your debit card. If the phone says it is your bank, most people will believe it.

Social media platforms must remove fake accounts and fraudulent ads more quickly. The Wall Street Journal recently documented how fake investment promotions on Instagram and Facebook have cost consumers their life savings. Banks regularly flag these scams, but takedowns are slow and inconsistent.

The Postal Service must strengthen protections against check theft, which remains one of the fastest growing forms of fraud and law enforcement needs more resources to investigate and prosecute cases, because no amount of bank investment can replace the deterrence of putting criminals behind bars.

We urge Congress, the administration, regulatory agencies, and others in the private sector to help close these gaps.

First, the administration should create a White House Office of Fraud and Scam Prevention to coordinate Federal efforts, unify consumer reporting, and drive a national strategy.

Second, we should require telecom accountability by closing loopholes that allow spoofed calls and texts, ban subscriber identity module (SIM) boxes that send thousands of scam texts, and ensure caller ID cannot be faked.

Third, we need to hold social media companies responsible by mandating quick, free takedown of impersonation accounts and impose liability if platforms knowingly allow them to remain.

Fourth, we must support law enforcement by providing for State-level financial crimes units modeled on Texas's Financial Crimes Intelligence Center, which has proven effective.

Fifth, we need to improve information-sharing by creating safe harbors for banks and regulators to exchange fraud data and require the Federal Communications Commission (financial) to establish a searchable spam text and messaging database.

Finally, we need to continue to combat check fraud by supporting the development of a national check verification system to authenticate checks at deposit.

Banks are proud of the role we play in protecting consumers. We continue to invest, to innovate, and to educate. ABA has launched several national anti-fraud campaigns, including "Banks Never Ask That" and "Practice Safe Checks" to help people recognize scams,

as well as “Safe Banking for Seniors” to help combat the ever-growing problem of senior fraud but unless every player in the fraud ecosystem accepts their responsibility, criminals will continue to victimize Americans at an unprecedented scale. Fraud is not just a banking problem; it is an ecosystem problem and until all parts of that ecosystem are equally committed to protecting consumers, the American public will remain at risk.

Thank you, and I look forward to your questions.

[The prepared statement of Mr. Benda follows:]

September 2025

Testimony of
Paul Benda
On Behalf of the
American Bankers Association
Before the
Subcommittee on Oversight and Investigations
Of the
House Financial Services Committee
September 18, 2025



American
Bankers
Association®

Testimony of
Paul Benda
On Behalf of the
American Bankers Association
Before the
Subcommittee on Oversight and Investigations
Of the
House Financial Services Committee
September 18, 2025

Chairman Meuser, Ranking Member Green, and members of the Subcommittee, thank you for the opportunity to offer testimony for today's Hearing entitled: "Fraud in Focus: Exposing Financial Threats to American Families." My name is Paul Benda, and I am the Executive Vice President of Risk, Fraud and Cybersecurity for the American Bankers Association (ABA)¹ and also serve as the Chair of the International Banking Federation Scams and Fraud Working Group as well as sit on the Advisory Board of the Global Anti Scam Alliance. At ABA, our members know that fraud takes a financial and emotional toll on their customers and banks of all sizes are making extraordinary efforts to protect and safeguard customer accounts as fraud has become more sophisticated.

Introduction

From using breakthrough technologies such as generative artificial intelligence (AI) to old fashioned theft of checks out of mailboxes, bad actors are relentlessly pursuing numerous ways to scam consumers and small businesses out of their money. Banks have a long history of improving and innovating to protect their customers—from the adoption of chip-enabled credit cards to multi-factor authentication to protect user accounts to the use of advanced AI tools to warn customers about potentially fraudulent transactions—banks have been on the front lines of innovation and deploying advanced capabilities to protect their customers. However, the fight against these criminals is one that banks cannot win on their own.

Unfortunately, bad actors are innovating, too. An example of widespread fraud efforts occurred when criminals took advantage of the economic devastation of Covid-19 and the unprecedented government response to support small businesses and out-of-work Americans. By the government's own estimate over \$300 billion² was lost, fueling the growth of more organized and sophisticated networks of financial criminals who continue to look for new ways to keep the

¹ The American Bankers Association is the voice of the nation's \$25.0 trillion banking industry, which is composed of small, regional and large banks that together employ approximately 2.1 million people, safeguard \$19.7 trillion in deposits and extend \$13.1 trillion in loans.

² See: <https://www.sba.gov/sites/sbagov/files/2023-06/SBA%20OIG%20Report%202023-09.pdf>

illicit funds flowing.³ The criminals are now using the tools, the personal information they stole and bought, and networks they built during the pandemic, along with secure messaging technology, to share tactics, techniques and procedures to expand their reach, finding new people to cash stolen checks and provide “mule” bank accounts⁴ to receive and move the funds. They are also becoming more sophisticated, using new advanced deepfakes.

Combating these criminals requires not just banks to act but all entities involved in the scam and fraud ecosystem. It’s imperative for the telecommunications companies and their regulators to take action to prevent criminals from spoofing legitimate names and phone numbers to convince customers they are speaking with a bank. Also, social media companies should take steps to proactively root out accounts pretending to be bank employees or financial advisors to convince people to put their money into their investment scams. In addition, the postal service must improve the security of the mail system so that when someone mails a check, it will not get intercepted, stolen, altered or cashed by the criminal.

Most importantly, banks need strong partnerships with law enforcement. These criminals cannot be stopped by banks alone, and we support law enforcement as they combat this scourge. While banks need to have the technology and infrastructure in place to defend themselves and their customers, they can only provide the leads necessary for law enforcement to track down the perpetrators. Law enforcement must have resources adequate to address the size of the problem, and we must have ways of addressing foreign bad actors who operate outside U.S. jurisdiction. Offenders cannot be allowed to continue to steal from American consumers and businesses. Banks also welcome the chance to partner with community-based organizations that are doing critical work in this area, as they are trusted voices in many underrepresented communities.

Banks clearly play a key role in fighting fraud, but unless every player in the ecosystem joins the fight, criminals will continue to steal at a scale we have never witnessed before.

State of Fraud Today

Banks have made significant progress in protecting themselves and their customers from being hacked. One recent industry analysis found that Financial Services, which is a category that includes more than just banks, accounted for only 7.7% of ransomware attacks in Q2 2024.⁵ Unfortunately, consumer losses from scams and fraud have been significantly increasing. Reliable data on consumer fraud is scarce, but the Federal Bureau of Investigation’s (FBI) Internet Crime Complaint Center (IC3) is the nation’s hub for businesses and consumers to report cybercrime and elder fraud.⁶ This data is limited to certain types of fraud, and therefore

³ <https://www.sba.gov/sites/sbagov/files/2023-06/SBA%20OIG%20Report%202023-09.pdf>

⁴ Money mules are people who, at someone else’s direction, receive and move money obtained from victims of fraud, technologies to change their voice and appearance in real-time video calls to execute romance and impersonation scams. A significant portion of the \$300B that was stolen during the pandemic has been reinvested by these criminals to create a highly advanced and sophisticated adversary who is a far departure from the basic phishing scams of yesteryear.

⁵ <https://www.coveware.com/blog/2025/7/21/targeted-social-engineering-is-en-vogue-as-ransom-payment-sizes-increase>

⁶ See, www.ic3.gov

under-reports the true dollar amount of fraud perpetrated, but it is still a useful proxy to identify trends and compare the number of different internet-based scams.

In the IC3's 2024 Internet Crime Report ("the Report"), released in April 2024, data showed a nearly 33% increase in losses reported by consumers and businesses from 2023 to 2024.

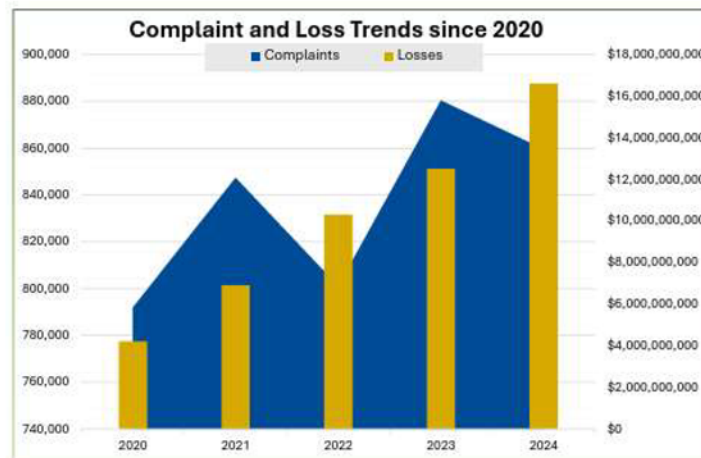


Figure 1. Complaints to IC3 over the last five years.⁷

According to the Report, the top three categories of scams in order of victim losses were investment scams, business email compromise, and technical support scams.

The Federal Trade Commission (FTC) also publishes the Consumer Sentinel Network Data Book⁸ on an annual basis that attempts to quantify the amount of fraud being experienced by consumers. Their trendlines are similar to those reported by the FBI and show an increase of 25% from 2023 to 2024 with losses in 2024 of \$12.5 billion. Unfortunately, neither the FBI nor the FTC have an accurate accounting of the total amount of fraud experienced by consumers. The FTC attempted to estimate the total amount of fraud due to potential under-reporting in 2023 and estimated total losses could be as high as \$158.3 billion⁹.

The lack of accurate data makes it difficult to accurately quantify the impact of fraud on Americans—it can be anywhere from \$12 billion to nearly \$160 billion. It is likely closer to

⁷ https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

⁸ https://www.ftc.gov/system/files/ftc_gov/pdf/csn-annual-data-book-2024.pdf

⁹ Page 12 - https://www.ftc.gov/system/files/ftc_gov/pdf/federal-trade-commission-protecting-older-adults-report_102024.pdf

\$100 billion than it is to \$10 billion, with Nasdaq estimating fraud losses in the Americas (North and South America) at \$151.1 billion¹⁰ in 2024.

The FBI showed a 33% increase in reported fraud by consumers, and the FTC showed a 25% increase year over year. It is clear that fraud is a huge problem that is growing bigger every year and yet there is no central reporting mechanism, no data source that can accurately track the total amount of fraud being experienced, and no single government entity responsible for protecting Americans from the massive thefts of wealth that are taking place on a daily basis. If we cannot accurately measure the fraud that's occurring, the types of attacks taking place, how can we hope to effectively combat it?

One thing is clear from the data; the criminals have shifted their tactics from brute force attacks and account takeover schemes to focus on imposter scams that build trust with the consumer and convince them to authorize the transfer of funds. The 2024 FTC Data Book listed imposter scams as the number one reported fraud category, more than twice as high as the second highest category.

The FBI's top reported fraud loss categories, investment scams, business email compromise, and technical support scams, are all types of imposter scams. Imposter scams can take many different forms, including a criminal pretending to be a financial advisor or romantic partner attempting to convince someone to invest in the next "can't miss" opportunity, or a criminal who has hacked a realtor's email account and then convinces the buyer to change the wiring instructions for the home closing costs. All of these scams depend on the criminal building trust with their victim. In fact, one publication attempted to quantify the different ways that criminals convince their victims to go along with the scam.

They looked at ten different scam types and asked victims of scams how did the criminal gain your compliance—through threats or intimidation, promise of financial gain, or gain your trust? Far and away, the criminals built trust with their victims to gain their compliance, as can be seen in Figure 2.

¹⁰ <https://www.nasdaq.com/global-financial-crime-report>

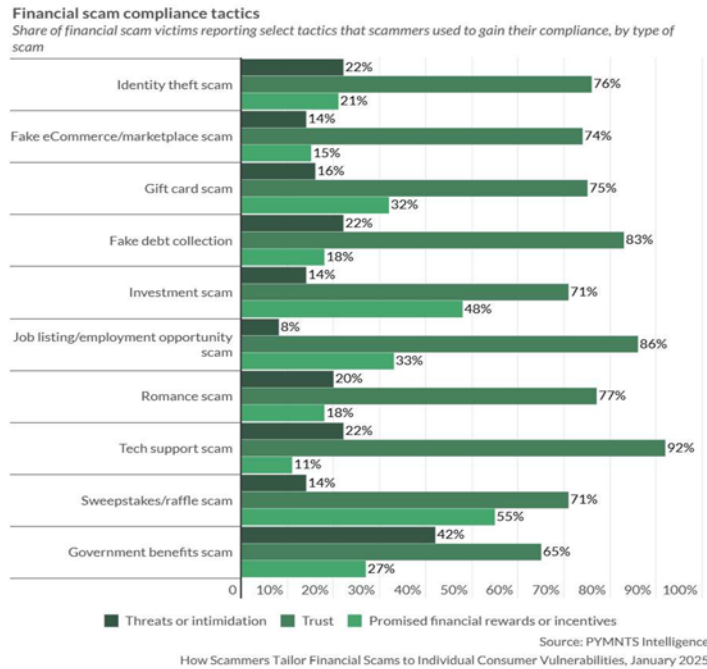


Figure 2. PYMNTS How scammers tailor financial scams to individual consumer vulnerabilities¹¹

This presents huge challenges for financial institutions. A cornerstone of our fraud education campaigns revolves around telling our customers not to send money to someone they don't know and trust, but for many scams, by the time that customer is ready to send that payment, they believe they know and trust who they're talking to. In fact, in many instances it can be challenging even for a family member to intervene and stop a loved one from sending funds to a scammer who has built trust over time, and it can be almost impossible for a bank teller to try to convince that person not to make the payment.

How does the criminal gain the victim's trust? Unfortunately, there are many contributing factors, from spoofed caller IDs that fraudulently show the name of a trusted entity such as a bank when it's actually the criminal calling; to social media posts and profiles that either impersonate trusted people or use stolen profiles to peddle different scams; to using stolen personally identifiable information to demonstrate to the victim that they must be from the bank

¹¹ https://www.pymnts.com/study_posts/how-scammers-tailor-financial-scams-to-individual-consumer-vulnerabilities/

(how else would someone know their name, address, last four of their social security number, etc.); to the skill of the scammer themselves who have practiced their lines on countless victims before and know all the right things to say to build rapport and trust with their victim. Looking at the myriad capabilities arrayed against the consumer and the industrial criminal complex in place to scam them, the question shouldn't be how someone fell for this scam. The better question is: how does anyone avoid becoming a victim when the deck is so stacked against them?

Combating imposter scams requires a whole of ecosystem approach, meaning each entity that is part of the scam lifecycle has a responsibility to protect the consumer and attempt to prevent the scam from happening in the first place. Telecoms have a responsibility to monitor their networks for scam activities and shut them down as well as ensure the fidelity of caller ID data. Social media companies should ensure that ads posted on their site are from legitimate businesses and shut down stolen and impersonated accounts. Financial institutions have a responsibility to monitor their payment networks for illicit transactions, stop them, and report the transactions to law enforcement. The government has a responsibility to create a national strategy to prevent scams and help coordinate activities across the ecosystem. The customer themselves have a responsibility to educate themselves about potential scams and learn about the tools and capabilities that could help them from being scammed. This type of shared responsibility model has been adopted in Australia and has shown significant promise. It is part of the reason that scam losses have decreased in Australia over the past year.

Though losses from the internet and imposter-based scams are most prominent, check fraud has become one of the fastest-growing categories of fraud impacting consumers across the country. Since the pandemic, check fraud has grown significantly and become one of the biggest drivers of fraud in the country. Unfortunately, just as there is limited data available for scam losses, the same is true for check fraud. Nonetheless, the scale of the problem can be seen with the number of Suspicious Activity Reports (SARs) filed with FinCEN that identify possible check fraud. In 2021, financial institutions filed more than 350,000 SARs to FinCEN to report potential check fraud, a 23 percent increase over the number of check fraud-related SARs filed in 2020. This upward trend continued into 2022, when the number of SARs related to check fraud reached over 680,000, nearly double the previous year's amount of filings.¹² The absolute value of check fraud occurring is unknown, but Nasdaq estimated check fraud losses in the Americas (North and South America) at \$21 billion¹⁰.

Even though the exact dollar value of fraud being committed cannot be determined, the trends are clear and troubling. Fraud is increasing across all channels. Banks are investing heavily in new technologies and capabilities to try to stop it, but when customers are convinced into giving their money to criminals or mail gets stolen from a post office, there are limits to what banks can do.

Attacking these trends requires work in the following areas:

¹² Subsequently, that rate has held fairly steady through 2024 with 662,000 check fraud SARs filed, potentially as a result of the law enforcement and regulatory resources focused on check fraud. See <https://www.fincen.gov/reports/sar-stats>

- *Develop a National Strategy to Prevent Fraud and Scams* – The scale of fraud being experienced is a national security threat and should be treated as such with a whole-of-government effort to prevent scams and fraud.
- *Close Loopholes to Stop Impersonation Scams* – Too many loopholes, such as phone number spoofing, exist allowing criminals to impersonate legitimate businesses and agencies.
- *Enhance Collaboration with Law Enforcement and Regulators* – Law enforcement plays a critical role in stopping fraud and ensuring perpetrators are prosecuted and prevented from further activity. Regulators can see patterns and trends that individual banks cannot.
- *Improve Information Sharing* – Criminals have an active information sharing ecosystem that banks and the public sector must match to try to slow the flow of illicit funds.
- *Continue to Enhance Banks' Anti-Fraud Operations* – The scale of fraud being experienced may make existing procedures and policies obsolete, and banks must continue to look for ways to improve bank to bank recoveries and customer experiences.
- *Increase Consumer Education* – Securing someone's account doesn't help if they can be convinced to willingly hand over their money or their login credentials.

Development of National Strategy to Prevent Fraud and Scams

While many of the funds stolen through scams and fraud go to U.S.-based criminals, large amounts are being transferred overseas. Fighting fraud is not only a priority to protect Americans from losing money to criminals, but also essential to protect national security. The lack of a centralized fraud response and tracking capability within the U.S. Government hinders the ability to spot trends, track tactics, techniques and procedures, and the ability to prevent fraud from occurring and to recover funds for Americans when fraud has been identified.

We believe that an Office of Scam and Fraud Prevention should be established within the Executive Office of the President to coordinate interagency efforts, streamline consumer reporting processes, and develop a national scam and fraud prevention strategy that involves both the public and private sectors.

Changes are Needed to Stop Impersonation Scams

Criminals' ability to impersonate legitimate businesses or government agencies is a major challenge that needs to be addressed to prevent the criminals from building trust with their potential victims and to break the scam cycle before it gets started. The challenge can be made more difficult when criminals are able to misrepresent themselves either through a spoofed caller ID that shows a legitimate business name and business' phone number, or through stolen or copycat social media accounts that are indistinguishable from real accounts. Currently technology can help criminals impersonate legitimate actors through three primary channels:

Spoofing of Caller ID – Currently there is very little oversight of the ownership of companies that can register as a telecom to authenticate calls and the numbers that are displayed on a caller ID. Unscrupulous actors have created a business model out of enabling criminals who have figured out loopholes that allow them to “spoof” the numbers and names of legitimate businesses with intent to defraud the call recipient. For example, banks have reported that customers have received calls that show they originate from the 1-800 number listed on the back of their debit card. When a customer is presented with what they believe is technologically validated information, it significantly aids the criminal in convincing the customer that the criminal is actually an employee of the customer’s bank.

Impersonation Text Messages – Criminals can use email-to-text tools to create text messages that look like they come from a bank or simply use similar numbers and formats to pretend they are from a bank. These can include links to fake bank websites, call back numbers, or prompts that cause the criminal to call the customer to socially engineer them to give up security credentials or send money from their accounts. In addition to email-to-text messages, criminals are making more use of “SIM boxes,” which are devices that allows the use and management of hundreds of SIM cards at once and enables the criminal to send thousands of scam texts in a short period of time. Other jurisdictions have banned SIM boxes. The United States should follow suit or at a minimum telecoms should monitor their networks for this type of activity and be given the authority to shut them down when they are used for fraudulent purposes.

Stolen or Spoofed Social Media Accounts – The FBI reported that investment scams had the highest losses in dollars of all scam types reported. There are many ways these scams can be perpetrated but one recent example is the unknowing takeover of actual bank employees’ social media accounts, which were then used to reach out to their connections to convince them to invest in fraudulent investment scams.

Spoofing of Caller ID Information

The Truth in Caller ID Act should be updated to clarify that it is illegal to spoof numbers you do not own or control. The law’s current prohibition—that it is illegal to spoof numbers with the “intent to defraud” —requires the government to prove that the bad actor intended to defraud the call recipient, which can be difficult to show. The FCC should be directed to increase enforcement and penalties against actors, including telecoms, that enable criminals to spoof the numbers and names of legitimate businesses on recipients’ Caller ID displays when telecoms fail to implement adequate “Know Your Customer” authentication procedures.

In addition to updating the Truth in Caller ID Act, policymakers should take the following steps to prevent criminals from using our calling network to place illegal calls:

- Set a date certain by which voice service providers of TDM networks must convert their equipment to IP. The existing “STIR/SHAKEN” call authentication framework requires calls to be signed at origination and attested through the call pathway until the call reaches the recipient. But STIR/SHAKEN only works over IP networks. If a call passes through a non-IP framework, the STIR/SHAKEN attestation is dropped. There is evidence that criminals exploit this gap to perpetrate fraud on consumers. Setting a date

certain by which voice service providers of TDM networks must convert their equipment to IP would expedite telecoms' work to transition all networks to IP.

- Require voice service providers that use a non-IP network—i.e., a legacy Time Division Multiplexing (TDM) network—to implement a caller ID authentication framework for that non-IP network. The public should not wait for voice service providers to transition all non-IP networks to IP. Providers should implement a caller ID authentication framework for that non-IP network without delay.
- Prohibit voice service providers from displaying data on the consumer's caller ID device when the authenticity of calls cannot be adequately verified through a direct and verified relationship with the call originator. If a voice service provider delivers to the consumer a call with unauthenticated or falsified Caller ID information, it should state "Unknown Caller" or similar cautionary information in the caller ID display. This will make clear to the recipient that the call is highly likely to originate from a person that is illegally posing as a government or business.

It is well documented that a significant number of scams originate overseas. These criminal enterprises leverage lax controls at telecom companies allowing them to change their Caller ID display number to look like the criminal's unauthenticated call originated within the U.S. Several other countries (United Kingdom, Australia, Germany, etc.) automatically block incoming international calls that attempt to spoof their Caller ID displays. The U.S. should implement a similar capability to block unauthenticated calls. A focus on blocking unauthenticated calls would ensure that legitimate U.S. businesses that place authenticated calls from call centers overseas can display the appropriate Caller ID information and complete their calls to U.S. consumers.

Impersonation Text Messages

There is a persistent and growing concern that SIM Boxes or "SIM Farms" are being used to facilitate text phishing campaigns. SIM boxes are technical devices capable of holding multiple SIM cards enabling criminals to send scam texts to thousands of people at once. Some banks are experiencing over 300% growth in phishing messages. There are very few legitimate uses of SIM boxes, and the U.S. should follow the lead of the U.K. who in April 2025 banned the possession or supplying of SIM boxes. In addition to banning these devices, the FCC should require all telecoms to implement enhanced filtering and detection controls to identify and mitigate when SIM boxes are used and implement enhanced fraud controls to identify criminal actors at account origination.

The FCC should establish a centralized database of customer-reported "SPAM" messages—i.e., suspected fraudulent or spam messages that customers report to their telecom or messaging provider through the "Report Junk" feature on iPhones and "Block and report spam" option on Android devices. The database should allow registered companies, including banks, to review the submissions for brand impersonation so that they can identify ongoing scams. This would allow the company to take action to mitigate the impact on their customers. Additionally, a centralized portal with contributions from telecoms and all significant messaging providers would provide real time intelligence in ongoing scam activities, allowing affected industries to

better respond with tailored mitigation measures. Importantly, all messaging providers—e.g., telecoms, Apple, WhatsApp, etc. —should be required to submit customer-reported “spam/scam texts/messages” to the database.

In addition to establishing a database of reported “SPAM” messages, these other text-based mitigation measures should be considered:

- Require subscribers to opt into “email-to-text” before receiving these messages. Criminals distribute large volumes of “smishing” messages (a “phishing” attack through text message) from e-mail addresses, which convert the e-mail message to an SMS text message. Bad actors often send these “e-mail to SMS” messages from telephone numbers that cannot accept incoming calls. These numbers are not uniquely assigned to an email address, and therefore, they cannot easily be reported and shut down. Requiring mobile wireless providers to offer email-to-text as an opt-in service would significantly reduce the use of this technology to send illegal text messages.
- Require text messages to be authenticated and set a deadline for the development and mandatory implementation of a text message authentication solution.
- Require originating mobile wireless providers to investigate and potentially block text messages from a sender after the provider is on notice from the FCC that the sender is transmitting suspected illegal texts. Criminals frequently use multiple numbers from which to originate texts. Originating providers are well positioned to stop illegal texts from a source because they have visibility into all text messages that a particular source is sending—not solely text messages from a particular number. (Terminating providers already are subject to a requirement to block all texts from a particular number when notified by the FCC of illegal texts from that number.)

Protect Banks’ Ability to Send Fraud Alerts

Banks send fraud alerts (also known as “suspicious activity alerts”) to a customer when the bank suspects that a bad actor has gained access to the customer’s account, such as through a stolen credit card, and is attempting a transaction on the customer’s account. Fraud alerts play a critical role in thwarting attempted fraud against customers. However, a rule issued by the FCC in 2024 – and set to take effect this coming April – could effectively require banks to cease sending fraud alerts to certain customers.

Under the Telephone Consumer Protection Act, with limited exceptions, a bank or other business can place an autodialed or prerecorded voice call or text message only with the prior express consent of the called party.¹³ A called party has the right to revoke his or her consent to receive these calls. In 2024, the FCC issued an order that requires a business that receives a text from a consumer (i.e., “stop”) in response to one type of message to stop receiving *all* future communications from that business by phone or text on unrelated matters – even if that was not the consumer’s intent (the “revoke all” rule).¹⁴ Thus, a consumer’s “stop” text message sent in

¹³ 47 U.S.C. § 227 *et. seq.*

¹⁴ *In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, Report and Order and Further Notice of Proposed Rulemaking, 39 FCC Rd 1988 (2024).

response to an autodialed past-due message could lead the bank to opt the customer out of all consented-to messages from the institution, including fraud alerts. This could result in increased fraud perpetrated against the customer. ABA urges the FCC to initiate a rulemaking to revise or rescind the “revoke all” rule.

Stolen or Spoofed Social Media Accounts

Criminals also target consumers by stealing personal social media accounts of employees of legitimate businesses or building fake accounts that portray them as working for that business. In both instances, the brand of the company, often a bank, is used to grant legitimacy to the criminal’s posts or messages. While this is a complex problem to combat and prevent, once these “impersonation accounts” are identified there should be a simple, quick and free method to request that they be taken down. Unfortunately, no major social media company offers such a method.

ABA strongly urges policymakers to ensure that social media companies provide a method to report impersonation accounts that is free to access and to use, and that results in an expedited removal of the offending account. Additionally, we recommend that if the hosting company refuses to take down the impersonation account, they then may be held liable for any fraud committed by that account as they are clearly providing the “means and instrumentalities” and have knowledge that the account is engaged in fraud.

Banks are committed to protecting their customers’ data and money. Our goal is to provide a safe and sound financial system that allows our customers to achieve their financial goals. Banks spend billions of dollars a year on cyber security and anti-fraud measures to provide one of the most secure banking systems in the world, but banks cannot do it alone. The technology companies that enable criminals to pose as trusted agents must help as well. The criminals have realized the challenges in directly hacking someone’s bank account, so instead they focus on convincing customers to give them that access. This is made easier when a phone, text message or social media site tells a consumer they are speaking with a banker and not the criminal behind the screen.

Partnership with Law Enforcement and Regulators

As I have discussed, the rising tide of fraud cannot be fixed by banks or technology alone. At some point, the criminals executing this fraud need to be caught, prosecuted, and sentenced so that they no longer commit these crimes. ABA has a history of partnering with law enforcement and the public sector on education and outreach activities along with identifying potential improvements in addressing fraud. We continue to work with our law enforcement partners and regularly connect law enforcement with banks to try and aid in the recovery of fraudulently transferred funds. Additionally, we are working to leverage existing reporting mechanisms of the IC3 to expedite the ability for banks to request another bank hold funds that were sent as part of a scam, but more needs to be done.

Law enforcement is a critical force in preventing and detecting fraud, and ABA applauds work by the FBI, United States Secret Service, and FinCEN to track and freeze funds that have been transferred fraudulently. The FBI IC3 Recovery Asset Teams have been great partners, but we

are concerned given the volume of fraud, that they may lack capacity to engage in lower dollar frauds that are reported to the IC3 portal. We would welcome a partnership with them to identify those cases that may not be pursued in a timely manner to determine whether a public-private partnership could be created to pursue those cases and result in more funds being returned to consumers.

Americans are losing billions of dollars to fraud annually. Yet, amid resource constraints and compelling demands, local law enforcement struggle to devote appropriate time and attention to these cases. Given the levels of fraud taking place against Americans, police departments and sheriff's offices should not have to choose between dedicating personnel to violent crimes and financial fraud cases. Additionally, law enforcement personnel need more effective training in addressing and responding to fraud allegations. Fraud is a continually evolving landscape and new fraud typologies develop each day. Enforcing the law and responding to these cases requires understanding the multifaceted strategies criminals employ to defraud Americans, particularly with respect to cybercrime. One state that has had success in engaging state and local law enforcement is Texas through their Financial Crimes Intelligence Center¹⁵. The Texas Financial Crimes Intelligence Center (FCIC) is the statewide fusion center that coordinates Law Enforcement Investigations for various types of Organized Financial Crimes.

While Federal law enforcement has a role to play in shutting down these scams, the volume of crimes being committed means that many cases reported to Federal authorities go uninvestigated and unprosecuted. Congress should establish a grant program for State and Local law enforcement to focus on financial crimes and scam response, enabling them to establish Financial Crime Intelligence Centers similar to the one in Texas. State and local law enforcement have close ties to their communities and can be nimbler in allocating staff to trending crimes.

Check Fraud and Partnership with U.S. Postal Service

Check fraud has increased significantly since the onset of the COVID-19 pandemic. In response, the ABA and member banks have made combating this rapidly growing threat a top priority, as criminal organizations increasingly rely on check fraud to perpetrate financial crimes. Check fraud schemes commonly begin with a theft of a check from the U.S. mail system, leading to check alterations and counterfeit checks created from the image of the stolen check. Criminals then move quickly from the point of theft to depositing the compromised check(s) into a bank account to steal money.

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

ABA and the U.S. Postal Inspection Service (USPIS) quickly recognized the need for cross industry collaboration to combat the growing wave of organized check fraud. In March 2024, the

¹⁵ <https://fcic.texas.gov/>

ABA and USPIS publicly announced a formal agreement to launch a joint Fraud Awareness Campaign. The joint initiative focuses on four main areas:

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

Through the partnership, we have placed a strong emphasis on training banks. ABA featured USPIS as a keynote speaker at its Check Fraud Symposium, which included banks of all sizes, industry vendors, and key government agencies. USPIS has also served as a valuable resource on approximately five ABA webinars and podcasts, enabling us to reach banks across the nation.

These speaking engagements have provided banks with critical insights into the importance of robust information sharing with USPIS, particularly in navigating a challenging prosecutorial landscape. As a result, banks have a clear understanding that check fraud investigations are a priority—and that the speed and thoroughness of their reporting significantly enhances the effectiveness of these investigations.

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

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

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

Improve Information Sharing to Combat Fraud

Given the massive scale and global reach of fraud, it is simply not possible for one bank to fight back alone; collaboration is required to ensure success. One of the most important tools banks have in combating financial crimes is shared information. However, due to inconsistencies across financial institutions, among other reasons, there are challenges in accessing actionable information in a timely manner.

That is why ABA has been working to establish a program to help banks share information that identifies activity that may involve terrorist financing or money laundering and deter crimes like fraud. ABA formed an association of banks to design and develop this new information-sharing exchange, which ABA will manage. The goal is to encourage the sharing of information in real-time so it can reduce the flow of funds to criminals' accounts and improve the quality of banks' reporting. We believe this effort can make a real difference in fighting fraud and other financial crime.

In addition to sharing information across financial institutions, the barriers to sharing information across industries including telecoms, social media, internet service providers and financial institutions should be lowered. The goal should be to prevent fraud from occurring in the first place, so real time information sharing is needed, but the regulatory hurdles, both real and perceived, create disincentives. A safe harbor with appropriate privacy protections should be established for entities engaged in good faith efforts to combat fraud to allow proactive protection of consumers from criminals seeking to scam them.

While sharing of data between private sector entities in real time can help prevent fraud, the government must get better at using, and where appropriate, sharing the intelligence that financial institutions share with them via SARs. Using the FinCEN SAR Stats page and searching for the number of SARs filed in 2024 that relate to fraud turns up 2.2 million records. This means financial institutions file on average more than 6,000 SARs a day focused on fraud. This information and intelligence on fraudulent activity is kept exclusively in the domain of law enforcement and government regulators. To combat the criminals executing these fraudulent activities, government must get better at using, sharing and disseminating the information that the private sector provides. It is certain that some of the information in the SARs submitted, if shared in a timely manner with the right financial institution, could stop a fraud from occurring and stop a person from being victimized. Private sector institutions must get better at sharing between themselves, but the government has a responsibility to better utilize the vast amounts of information that the private sector shares with them with a goal of preventing the fraud.

Banks are Continually Improving Anti-Fraud Operations

The rise in fraud has not only impacted consumers but banks as well. The rise in the volume of cases, the complexity of processing check fraud claims, and the increasing capabilities of criminals with new tactics and technologies has created very significant operational challenges for banks both in combatting fraud and processing claims.

ABA and the banking industry are committed to improving their effectiveness fighting fraud and the experience of customers who experience fraud and scams. To that end, we have launched several initiatives to improve the overall process including:

- ABA established the Fraud Contact Directory. Surprisingly, there is no single resource that a financial institution can go to find a contact at another institution. ABA built this web resource starting with banks and focused on improving and accelerating the check fraud claims process. The effort has now expanded to offer contacts for all different kinds of fraud and has even been expanded to allow access to credit unions all at no cost to participants. This resource includes more than half of all banks in the country and is routinely cited by bankers as providing operational efficiencies as well as helping them recover fraudulently transferred funds.
- Treasury checks are sought after instruments by criminals due to the requirement that a significant amount of funds be made available the day after deposit. The Treasury Department hosts a public facing website called the Treasury Check Verification System (TCVS) that allows a bank to validate the check amount and check number, but unfortunately criminals figured out how to counterfeit Treasury checks and sell versions that are fake but also pass TCVS verification.
- To help address this issue, Treasury built a version of TCVS that also verifies the payee name but due to the sharing of personally identifiable information they did not allow its use through the public website but through a direct connection to Treasury systems. While this connection is free, it does require building of an interface to the Treasury system and onboarding with encryption keys. This process was challenging for some banks as well as for Treasury to try and interact with and distribute encryption keys to the 4500 banks operating in the U.S. To help alleviate these challenges, ABA built an interface to the Treasury Payee Verification TCVS system and hosts it on its website at aba.com/TCVS. This service is free for all ABA member banks and allows them to verify Treasury check details, including payee in real-time. Additionally, we are adding a capability for banks to report when a fraudulent check is found so we will be able to track in real time the level of fraud attempting to be perpetrated against banks. ABA fully supports the Administration's move away from paper checks, but we recognize that moving fully to electronic payments will likely take some time, and this effort will help prevent fraud during the transition. Since its launch in late June nearly 600 banks have logged onto the system and validated over 11,000 Treasury checks.
- Recognizing that check fraud is likely to be a continuous and ongoing problem, simply focusing on the claims process will not prevent the fraud from occurring. So ABA hosted a Check Fraud Summit with banks of all sizes, vendors and regulators and kicked off the National Check Verification Feasibility study. Currently no system exists for commercial/consumer checks like the TCVS system that can validate a check in real time at the bank of first deposit. This effort will explore the potential for development of a standard data file format that would allow existing positive pay vendors and potentially others to share the positive pay and payee positive pay data

recorded by banks which could then be queried in real time by the bank of first deposit to verify a check when it is initially presented for deposit. The initial idea is to build an information exchange that could be leveraged by multiple vendors to provide a capability and preserve competition and encourage vendor innovation. ABA plans to publish the results of the study in October 2025 and is actively exploring a pilot proof of concept with both bank and vendor participants.

- When a scam does occur, time is of the essence, both for the victim to report it and for the bank and/or law enforcement to take action. ABA has launched an initiative that augments existing payment rail recall procedures by attempting to develop a standardized process how banks can notify each other when a fraudulent transaction has been sent, how a customer can report and attest fraud has occurred, and how banks can quickly provide the required legal assurances that the funds can be returned. Currently this process can vary bank by bank but by creating a standardized framework, having outside counsel review the policies and procedures to ensure compliance with laws and regulations, and leveraging the contacts in the ABA Fraud Contact Directory, we hope to accelerate the timelines these hold requests can be sent and acted upon to “catch” the funds before they can be cashed out or sent to overseas banks that may not be cooperative in returning the funds.

In addition to the rise of scams and fraud affecting Americans of all ages, elder financial exploitation, defined as the illegal or improper use of an older adult’s funds, property, or assets, is occurring at unprecedented levels. According to AARP, the average loss per victim is approximately \$120,000, while the FTC estimates total annual losses of older Americans to be as high as \$61.5 billion when accounting for underreporting. These crimes not only devastate individuals and families but also erode trust in financial institutions and place a growing strain on social support systems.

In response, the banking industry has stepped up efforts to detect and prevent exploitation. Banks train staff to recognize warning signs, report suspicious activity, and work closely with law enforcement and adult protective services to investigate cases. They are also educating customers and communities about how to protect themselves and are leveraging technology to flag unusual account behavior. Despite these efforts, banks face hurdles that limit their ability to act swiftly and decisively when exploitation is suspected.

To strengthen these protective measures, the federal government should enact legislation authorizing banks to delay, hold, or freeze transactions when elder financial exploitation is suspected. This law should be modeled after FINRA Rule 2165, which allows securities firms to pause disbursements and transactions to protect vulnerable clients. A national standard would give depository institutions the legal protection they need to take preventive action without fear of liability. It would also close gaps between varying state laws, enable earlier interventions, and ultimately provide stronger, more consistent safeguards for older Americans.

Banks Provide Extensive Consumer Education

Consumers are on the front lines of this fight, and we need to do all we can to ensure they have the tools and knowledge they need to protect themselves. We are proud to report that banks of all sizes have significantly increased their education of customers in recent years in addition to investing billions in fraud fighting technology and tools. For example, many banks routinely provide tips for spotting scams in branches, customer communications, and websites and provide timely warnings that customers do not share passcodes or send money to people they do not know. Many banks also bolster their individual fraud-fighting efforts by participating in ABA's industry-wide consumer education efforts.

However, while banks can help to keep customers' accounts secure, these controls can be defeated if a criminal convinces the customer to let them into the customer's account or to send them money. Ultimately, banks have little power to stop customers from withdrawing their own money, and indeed victims often are coached to ignore the bank employees who warn them not to withdraw or send the money. People need to hear from other sources as well, and ABA encourages other trusted sources, such as government agencies or nonprofits, to partner with us to amplify the important work banks are doing to educate consumers about fraud.

Stopping Phishing

One of ABA's most important consumer protection initiatives is our award-winning #BanksNeverAskThat¹⁶ anti-phishing campaign. Since its launch in October 2020, we have helped educate millions of consumers on how to spot common scams from bad actors posing as their bank.

This public awareness campaign educates consumers by posing ridiculous questions banks would never ask a customer. Using humor, bold graphics, videos, an interactive quiz, and an educational video game, we drive home the message that your bank will also never contact you asking for sensitive personal information such as your password, pin or social security number. ABA provides all campaign materials free of charge to all banks, so they can deliver the #BanksNeverAskThat messaging in their local markets.

To date, more than 2,500 banks have participated in the #BanksNeverAskThat campaign and spread its educational content to millions of Americans through social media, bank websites, ATM screens and bank branches across the country. ABA has also promoted the campaign nationally through television and radio ads. In the Washington area, anyone who has been to a Washington Capitals, Wizards or Nationals game has probably seen its educational message. A Spanish language version of the campaign is also available at: www.BancosNuncaPidenEso.com

¹⁶ www.banksneveraskthat.com

ABA National Consumer Campaign to Combat Check Fraud

Building on the success of the “#BanksNeverAskThat” anti-phishing campaign, the ABA also launched “#PracticeSafeChecks,” campaign in 2024. Partnering with more than 1,600 banks across the country in its first year, the campaign educates consumers on how they can protect themselves against check fraud and encourages the use of more secure digital banking tools to send money.

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

ABA provides all campaign materials free of charge to member and non-member banks, allowing participating institutions to customize and deploy the content in ways that best serve their local communities, while consumers can also find the helpful tips by visiting www.PracticeSafeChecks.com and our Spanish language website www.CuidaTusCheques.com. Both the #PracticeSafeChecks and #BanksNeverAskThat campaigns will relaunch on October 1 with new educational content for consumers. We would welcome and deeply appreciate any amplification of these important campaigns by members of Congress and their offices.

Combating Elder Fraud

In addition to its public awareness campaigns reaching all consumers, ABA has active programs to specifically protect seniors from scams. Given the unique risks facing older customers, ABA works through its non-profit foundation to ensure that all banks, irrespective of membership status, can access tools and resources to prevent, detect, and combat elder financial exploitation.

The ABA Foundation is a 501(c)3 corporation that provides free programs and resources to help banks support the financial well-being of their customers and communities. The ABA Foundation offers banks free resources through the Safe Banking for Seniors program to educate their communities on materials to inform their communities about avoiding scam, preventing identity theft, and financial caregiving.¹⁷

Since 2016, more than 2,000 banks have participated in the ABA Foundation’s program. Banks use the materials to help empower their communities and lead workshops, post videos and other content on social media, and share vital information during one-on-one conversations with customers. All the resources are available at no cost to ABA member and non-member banks.

Through partnerships with the FBI, FTC, USPIS, and other federal agencies, the ABA Foundation has also developed infographics and tip sheets to raise awareness about: check theft scams, cryptocurrency investment scams, deep fake scams, fake check scams, government

¹⁷ <https://www.aba.com/seniors>

imposter scams, imposter scams, money mule scams, online dating scams, peer-to-peer payments, phishing scams, and tech support scams.¹⁸

While ABA's campaigns have made a difference in educating the public, we are just one voice. We really need a nationwide message coordinated among multiple agencies (including the CFPB and FTC), nonprofits, and the private sector to promote a simple and memorable action plan for people of all ages facing scams. The campaign should also focus on dispelling the behavioral techniques scammers use in impersonating authorities, indicating urgency, requiring secrecy, and manipulating people into action.

Conclusion

Banks are working every day to protect their customers from fraud by investing in new technologies, deploying public relations campaigns to educate consumers and small businesses about old and new scams, and partnering with law enforcement and other federal agencies on new initiatives to combat fraud. Yet our industry recognizes that there is more work to do, and banks cannot stop criminals by themselves. Every player in the fraud ecosystem must play a role; from the telecommunications firms to the social media companies to the Postal Service. And we would welcome collaboration with community groups who have the trust of consumers across the country. The goal of all banks is to help their customers have a safe and secure financial future, and ABA and the banking industry stand ready to work with all stakeholders to protect our customers from fraud.

Thank you once again for the opportunity to testify. I look forward to answering your questions.

¹⁸ <https://www.aba.com/protectyourmoney>

Chairman MEUSER. Thank you as well.

Mr. Bednowitz, you are now recognized for 5 minutes for your opening remarks.

**STATEMENT OF IAN BEDNOWITZ, GENERAL MANAGER,
LIFELOCK AT GEN**

Mr. BEDNOWITZ. Thank you.

Chairman Meuser, Ranking Member Green, and members of the committee, good morning, and thank you for this opportunity to testify on this critical topic of fraud affecting American families.

My name is Ian Bednowitz, and I am the general manager of LifeLock. LifeLock is the leading identity-theft protection service in the U.S. and LifeLock is part of a larger company, Gen, a global S&P 500 company that has over 500 million consumers that we protect through our brands NortonLifeLock and Avast.

Fraud today is not just growing; it is accelerating at an unprecedented rate. You know, multiple people have highlighted statistics. The statistics we have is that the American consumer lost \$16.6 billion in reported losses last year. That is a 33-percent increase year on year, and that translates into \$51 for every person in this country.

At LifeLock, we have sent over 81 million identity theft alerts, and the number of Social Security numbers that are on the dark web that are being exposed to breaches increased from 8 million to 300 million in just 1 year.

These are not just statistics. Behind these facts are seniors that are losing their life savings, are young people whose financial futures are ruined before they even start their careers, and families who are blindsided by fraud.

Fraud, unfortunately, does not discriminate. Young people get victimized more frequently because they are online more often, whereas seniors experience much larger fraud when it happens—or much larger losses. The average senior lost \$35,000 in reported fraud, and, in total, seniors lost a staggering \$5 billion.

Yet, despite these statistics, over two-thirds of seniors say that they feel invincible, that they feel safe from the risks of fraud and scams. This represents a huge disconnect between perception and reality and artificial intelligence is only increasing this gap. In the hands of criminal organizations, artificial intelligence is allowing them to industrialize fraud, allowing them to make phishing emails that are perfect, voice clones that are compelling, deepfakes that can fool even the most sophisticated American citizen.

AI, on the other hand, is also our best defense against these criminal organizations. At Gen, we use AI to go through millions and millions of data points to detect fraud in real-time. We use it to detect deepfakes and to protect consumers, to prevent scams from ever getting to consumers in the first place but technology is not enough. We also invest in education, in partnerships, and sharing intelligence with law enforcement.

Congress has a critical role to play in this fight. Based on our experience, we urge three primary priorities.

We have to stop fraud before it happens; raise awareness of the threats through national education campaigns that focus on scams,

fraud, identity theft; modernize breach notifications; and invest in public-private partnerships that raise digital literacy.

Two, we have to disrupt the scam supply chain. So the social media networks, the companies, the data brokers that trade in personal information that are fueling the rise of scams, we need to better regulate them and we need to empower our law enforcement to be able to go after international organizations across borders, give them the tools to be able to take down the infrastructure and to be able to collaborate across countries.

Then, third, we need to empower victims and support local law enforcement. Local law enforcement needs the education and the tools to be able to deal with these types of scams and fraud and victims need to be able to have a centralized repository of breaches and actions that they can take to remediate and address when they are victimized.

Fraud now represents a systemic threat to our digital economy and to the trust that consumers have in their digital lives. Together, government, industry, and civil society must work together and collaborate to protect American families, restore confidence, and secure the digital economy for every American.

Thank you, and I look forward to your questions.

[The prepared statement of Mr. Bednowitz follows:]



Testimony of Ian Bednowitz,

General Manager, LifeLock

A Division of Gen Digital, Inc.

House Financial Services Committee

Subcommittee on Oversight and Investigations

Hearing entitled: "Fraud in Focus: Exposing Financial Threats to American Families"

September 18, 2025

Testimony of Ian Bednowitz

My name is Ian Bednowitz, and I serve as General Manager of LifeLock, a leading U.S.- based identity protection brand. LifeLock is part of Gen (NASDAQ: GEN), a global consumer cyber security company trusted by approximately 500 million users worldwide to keep them safer online. Alongside LifeLock, you may also recognize our other flagship brands Norton and Avast, both with decades of experience combating cyber threats and protecting consumers.

Our consumers are protected by award-winning security products backed by a team of researchers and cyber experts that block billions of threats annually. Gen was an early adopter of AI to keep up with criminals and better protect our consumers. Today, we are building tools that use AI to detect AI threats, monitoring behavioral anomalies and fraud patterns.

Fraud is escalating at an exponential pace, putting more people at risk every single day. Reports show the number of Social Security Numbers (SSNs) exposed in data breaches and sold on the dark web has increased from 8 million before 2024 to over 300 million. In addition, last year, the IRS flagged nearly 2 million tax returns for possible identity fraud. Our own stats show that LifeLock sent more than 81 million Identity Theft Protection alerts and notifications in 2024 alone.

Recently the Global Anti Scam Alliance (GASA), reported that fraud and scams are now the fastest-growing consumer crime globally and in the United States, overwhelming enforcement systems and undermining trust in digital services. According to the FBI's Internet Crime Complaint Center C3 report [Internet Crime Complaint Center](#), Americans reported \$16.6 billion in fraud losses in 2024, a 33% increase from 2023, with over 850,000 complaints filed.

As staggering as those numbers are, we are seeing a seismic shift in the fraud landscape. Deepfake technology is now being used to steal even more money from people. Fraud is being industrialized through AI tools that exploit public trust and institutional weakness. Criminals that work in fraud and scams are building international networks that can operate as effectively as professionally run and structured businesses. The organized frameworks allow for scalability and cross jurisdictional operations that are difficult for law enforcement to address.

It is no longer what we used to think was a lone actor in a sweatshirt on a laptop in their basement. They have grown to become international crime rings. An [alert from FinCEN in late 2023](#) shows how sophisticated networks engaged in scams and social engineering and the growing threat of "Pig Butchering" are operating around the world.

Our own data shows over 75% of cybercrime originates from scams and social engineering, where cybercriminals manipulate people into giving money or personal information. These are not abstract numbers. They represent seniors who lose their life savings, young adults whose financial reputations are damaged before they even begin their careers, and hardworking families blindsided by criminal

schemes. Fraud has become a tax on trust, undermining both financial security and personal confidence in the digital economy.

High-Impact Scams and the Price Americans Pay

Americans are facing a surge in increasingly sophisticated fraud schemes, many backed by organized international crime rings. Some of the most common and costly scams include:

- **Identity theft** – criminals obtaining personal information about an individual from a combination of breaches, the public internet or even the individual him or herself and using it to steal money through tactics such as applying for loans or credit cards, seeking employment or stealing tax returns cost Americans [\\$23B in 2023](#).
- **Investment scams** – fraudulent investment opportunities, often exploiting cryptocurrency and digital platforms, cost Americans [\\$5.7 billion in 2024](#).
- **Imposter scams** – criminals posing as government agencies, banks, employers, or even family members drained nearly [\\$2.95 billion in 2024](#).
- **Job and business opportunity scams** – scams exploiting those seeking income or stability cost Americans [\\$751 million in 2024](#).
- **Online shopping scams** – fake websites and ads targeting consumers with undelivered goods cost Americans [\\$432 million in 2024](#).
- **Romance scams** – cost Americans [\\$1.14 billion in 2023](#), preying on trust and emotional vulnerability.
- **Pig butchering scams** – one of the most devastating trends, blending romance, investment fraud, and emotional manipulation; losses often reach tens or hundreds of thousands per victim.

Together, these scams paint a stark picture: from fake investments and romance swindles to everyday identity theft and online shopping fraud, Americans are losing billions each year to schemes designed to exploit trust, urgency, and financial vulnerability. Behind every dollar from the \$16.6 billion in fraud losses reported by the FBI in 2024 alone is a disrupted household, a stolen dream, or a family left picking up the pieces, underscoring the profound human and economic toll of modern fraud.

How Scams Work: Technology Meets Psychology

Fraud today is not just a technological problem; it is a psychological one. Criminals have learned to combine the precision of stolen data with the power of emotional manipulation. These scams are often triggered or amplified by emotionally charged events, a natural disaster like the recent floods in Texas or fires in California, a major political moment, or a sudden financial disruption. In those high-stress situations, people are more vulnerable to manipulation, and scammers exploit that urgency. Fraud tactics now rely just as much on emotional pressure as on technology, targeting individuals at their most vulnerable.

At the same time, the raw materials for fraud are everywhere. Billions of personal records circulate on the dark web, and an estimated 75% of Social Security numbers are already compromised. Much of this data is obtained through breaches and data brokers, while social media adds another layer. Every post, picture, or life update can give criminals the details they need to stitch together scams that feel authentic and personal.

Scammers then use this information in two ways. First, they can commit identity theft, posing as the victim to open credit cards, take out loans, or even apply for jobs in their name. Second, they can use the same personal data to target the victim directly, sending scam messages or calls that appear to come from a bank, a lender, a government agency, or even a trusted family member.

Artificial intelligence has made both approaches easier and more convincing. AI tools can generate polished phishing emails in seconds, automate scam operations at scale, and even create realistic audio or video “proof” that what the victim is seeing or hearing is legitimate. Deepfakes take this one step further: a cloned voice that sounds like a panicked child asking for money, or a manipulated video of a familiar face, can trick even the most cautious person into sending personal information or transferring funds.

This combination of breached data, emotional pressure, and AI-driven deception has made fraud harder to detect and far more dangerous. It is no longer just about spotting a misspelled word or a suspicious email. Today’s scams are designed to bypass both technical safeguards and human instincts, leaving people exposed in ways that feel deeply personal.

Who’s Being Targeted

Fraud does not discriminate, but its impact varies by age group. Gen’s internal research shows that in 2025, 35% of Americans have already been targeted by a scam, well above the global average of 24%. Among those targeted, nearly three-quarters suffered financial harm, losing an average of \$3,858, with some individual losses reaching as high as \$149,000.

Younger adults are reporting scams at higher rates than older generations, according to FTC Sentinel data, often because they spend more time online and are more likely to trust digital platforms. But older adults, once victimized, lose far more. FBI Internet Crime Complaint Center (IC3) data shows the average reported loss for seniors is over \$35,000, a devastating blow for those relying on retirement savings. In fact, seniors reported nearly 150,000 complaints in 2024, with total losses reaching almost \$4.9 billion. Families across the country recognize the danger: according to Gen data, 59% say an older loved one has already been scammed, and another 71% are worried they will.

These numbers tell a clear story. Scammers adapt their tactics to exploit people’s unique vulnerabilities, whether it’s the digital exposure of the young, or the financial stability and trust of the old. Emotional manipulation is proving to be just as powerful a weapon as technical exploitation.

Areas of Fastest Growth

What is most concerning is not only the scale of fraud, but the rate at which it is accelerating and the way criminals are organizing themselves to industrialize these crimes.

Recent research confirms this trend. A study published by [Cornell University](#) on pig-butcher scams found that these scams follow a structured lifecycle: building trust, luring victims into fake platforms, and coercing ever-larger investments. Far from casual or opportunistic, these schemes are coordinated enterprises with specialized actors managing different stages of fraud.

Meanwhile, in the second quarter of 2025, the [Gen Threat Report](#) showed a 340% quarterly increase in the risk of being impacted by a financial scam. The increase in scams affected both desktop and mobile devices, the latter largely fueled by ads on social media where scammers lure their victims into fake messages and even false ads for sites that promote helping people fight scams.

The Identity Theft Resource Center's (ITRC) 2023 [report](#) documented a 118% increase in job scams and a surge in misuse of compromised credentials, including systematic abuse of tools like Google Voice. This illustrates how criminals scale identity theft across thousands of victims using repeatable methods.

Industry studies also link fraud to organized criminal rings. The [Onfido 2022 Identity Fraud Report](#) found a 57% rise in document fraud, connecting forged IDs and synthetic identities to organized groups that create fraudulent accounts for money laundering and other downstream scams.

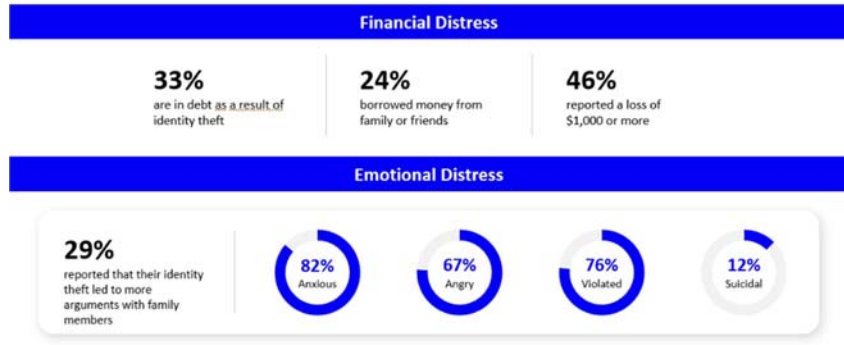
Taken together, these findings demonstrate why scams are accelerating so quickly. They are no longer isolated incidents but repeatable, scalable, and global operations, built on specialization, technology, and coordination. Three forces are fueling this growth: the flood of breached data, the use of AI to supercharge fraud, and the emotional manipulation that makes scams so effective. Together, they create a fraud economy that grows faster each year: more pervasive, more sophisticated, and harder for people to recognize and prevent.

The Human Impact

For every statistic, there is a family living through the fallout. Fraud victims lose retirement savings, homes, and financial stability. Many carry the weight of shame, isolation, and fear, which too often prevents them from reporting what happened. Families are forced to step in, not only to help recover stolen funds, but also to repair the emotional toll.

Identity theft victims often describe it as a lingering violation – a loss of control that doesn't end once the money is gone. Fraud is not just about money; it undermines people's confidence in technology, institutions, and the bonds of trust that hold families and communities together. The data bears this out: according to the [2024 Identity Theft Resource Center Consumer and Business Impact Report](#), 33% of victims end up in debt, 24% borrow money from family or friends, and nearly half (46%) lose \$1,000 or more. Beyond finances, 29% say identity theft caused more family conflict, while 82% report feeling anxious, 67% angry, and 76% violated. Most alarmingly, 12% said the experience left them feeling suicidal.

The impact on identity theft victims



These numbers make clear that fraud and identity theft are not abstract crimes but deeply personal crises that ripple outward. The human toll of fraud underscores why stronger protections and coordinated responses are urgently needed. Data alone cannot capture the full cost when victims are left in debt, families are fractured, and trust is eroded.

AI: A Dual-Edged Sword

Artificial intelligence is now at the heart of this battle, both as a weapon for criminals and as a shield for protection.

On one side, fraudsters are using AI to supercharge their operations. Phishing emails that used to be riddled with spelling errors are now flawless, tailored, and persuasive. Criminals can clone voices to sound like a distressed family member or manipulate video to impersonate a trusted official. These deepfakes make scams far more believable, stripping away the warning signs people once relied on to spot fraud. AI has lowered the barrier to entry, making it faster, cheaper, and easier for criminals to target more victims at scale.

But on the other hand, AI is also our greatest defense. At Gen, we have invested in building AI-powered protections that keep people safe in real time. Our Genie AI Assistant technology scans millions of messages and images, flagging scams before harm occurs. We've started integrating Deepfake Protection into our products, so people can identify manipulated content that might otherwise fool even the most cautious among us. Every day, our machine learning systems analyze billions of data points, detecting unusual patterns that signal fraud and shutting down threats before they spread.

The truth is simple: AI is a double-edged sword. If left unchecked, it will allow fraud to grow at an unprecedented scale. But when deployed responsibly, it becomes a shield that protects people from the very dangers criminals are trying to exploit.

Gen's Role and Response

At Gen, protecting people is not just our business, it is our mission. Across our family of trusted brands, including LifeLock, Norton, Avast, Avira, and AVG, we safeguard more than 500 million people worldwide. And we know that technology alone is not enough. Our approach combines protection, intelligence, and education.

- **Protection:** Through LifeLock, we provide identity monitoring, dark web alerts, and restoration services so people can recover quickly if their information is compromised.
- **Intelligence:** Our threat network processes billions of data points from hundreds of millions of devices, creating one of the most robust consumer-focused cyber intelligence systems in the world. That intelligence allows us to spot stolen credentials, fraud rings, and malware long before most people are even aware of the risk.
- **Education:** We invest heavily in awareness, from partnerships with the PTA to new training modules that teach families about AI safety. By equipping parents, teachers, and children with the knowledge to recognize scams, we break the cycle of silence and shame that so often leaves victims isolated.
- **Collaboration:** We share our threat and scams intelligence with law enforcement and policymakers, helping to disrupt criminal networks and inform strategies that strengthen consumer protections.

And behind each of these efforts are real stories. I think of the elderly man who was tricked into believing \$9,000 had been mistakenly deposited into his account and was pressured to return it through a Bitcoin ATM. Because he was a customer with one of our scam protection products, Genie Pro, he was able to file a police report and was reimbursed for his loss. Or the woman who avoided losing thousands on a fake shopping site because she followed her family's simple rule: before making an unusual purchase, check with a second trusted person first. That five-minute pause stopped her from entering her credit card details into a fraudulent site designed to steal them.

These stories remind us that while advanced technology is critical, sometimes the simplest protections, such as safe words, second checks, open conversations, can be just as powerful. That's why we call our model an **All of the Above+ approach**. It means using every available best practice but also going further: embedding protections directly into the products and services people use every day, and ensuring that when fraud or breaches occur, there are trusted solutions ready to restore confidence and minimize **damage**.

Policy Considerations: A Unified Response to a National Challenge

Protecting American consumers from digital fraud requires more than good intentions. It demands coordination between government, industry, and civil society. Based on Gen's threat intelligence and experience with millions of consumers, we believe there are three essential priorities for Congress to consider:

Prevent Fraud Before It Happens

Launch national public education campaigns that cut across age groups, platforms, and communities. These campaigns should provide plain-language guidance on identifying scams, especially for seniors and younger digital natives. Formalize public-private partnerships with schools, nonprofits, and consumer platforms to deliver digital literacy training, especially focused on AI scams and identity fraud. Modernize breach notification standards so that alerts are timely, understandable, and come up with clear next steps for affected consumers.

Disrupt the Scam Supply Chain

Enact stronger oversight of data brokers and digital intermediaries that traffic in the personal information used to build scam campaigns. These entities should be subject to clear accountability for how data is collected, sold, and secured. Equip federal agencies with targeted enforcement tools, including sanctions against known international scam networks and the ability to take down infrastructure tied to repeat offenders. Increase scrutiny of digital advertising platforms and telecom providers that allow fraudulent content to spread. These companies must do more to detect and disrupt scam campaigns before they reach consumers.

Support Law Enforcement and Empower Victims

Provide funding and training for state and local law enforcement to investigate digital fraud and identity theft. Many scams are international in origin, but the harm is local. Police departments need better tools and coordination to pursue these cases.

Establish a centralized clearinghouse for breach information and consumer remedies. Victims should not have to hunt for answers across dozens of sources when their data has been compromised. Set clear standards for consumer protection services, including identity monitoring, fraud remediation, and credit restoration tools. These services must be trustworthy, effective, and easy to access after a breach or scam.

Conclusion

The federal government has unmatched scale and policy reach. The private sector brings technical expertise and real-time threat data. Consumers face the consequences when those efforts do not align. We believe the time has come to treat fraud not as a series of isolated crimes, but as a systemic threat to national financial confidence and to act accordingly.

Chairman MEUSER. Thank you very, very much.
 Ms. Griffin, you are now recognized for 5 minutes.

**STATEMENT OF KATE GRIFFIN, DIRECTOR, NATIONAL TASK
 FORCE ON FRAUD AND SCAM PREVENTION, ASPEN INSTI-
 TUTE FINANCIAL SECURITY PROGRAM**

Ms. GRIFFIN. Chairman Meuser, Ranking Member Green, distinguished members of the subcommittee, thank you for inviting me.

My name is Kate Griffin, and I am director of the National Task Force on Fraud and Scam Prevention at the Aspen Institute Financial Security Program.

Over the last year, hundreds of experts from more than 80 institutions, public and private, have spent thousands of hours together to mount a coordinated defense against scams—the ability for criminals to deploy sophisticated social-engineering techniques that lure victims to send their hard-earned money.

As my colleagues have outlined, scams are a growing threat to all of society. Every day, roughly 50,000 Americans become victims. We believe one in five Americans have been affected to date and these people are young and old, urban and rural, rich and poor. Everyone is at potential risk.

Because of this, every week, more than \$2 billion is flowing out of American pocketbooks and into the hands of foreign criminal enterprises, who use those funds to fuel other illicit crimes, including drug and human trafficking. Research suggests that this scams industry now rivals the size of the illicit drug trade, and scam losses reported to law enforcement have more than tripled since 2019.

Those reports, though, are only a fraction of what is really happening. In fact, the FTC has estimated that actual fraud-related losses, accounting for this under-reporting, exceed \$158 billion per year.

The vectors of attack are varied, which is why we will talk about this as an ecosystem or whole-of-society problem. Scammers target victims on all of the core systems of American commerce and communication: telecoms, messaging, digital platforms such as social media or paid advertising, retail, and financial services spanning banking, payments, fintech, crypto, and investments.

Most U.S. adults report receiving scam messages through those means daily or weekly and those consumers are asking for your help. They do not know where to turn.

Being tricked by a scammer to send money or provide access to a financial account is the second-largest crime concern in the U.S., second only to identity theft. People are worried more about scams than they are about violent crime or burglary and they rarely report when it happens to law enforcement. In fact, most victims, 7 in 10, will report directly to their financial institution, while only a small fraction of that will report to local law enforcement or a Federal agency.

That is why preventing scams requires this whole-of-ecosystem response. Leaders in our task force are very sophisticated fraud fighters, but they are asking for help with scams. They have underscored the need for collaboration across all those sectors and the desire for strong leadership from the Federal Government in doing so. No single entity in the scam's lifecycle can do this alone.

We will have a detailed set of recommendations in a forthcoming report from the task force in a few weeks which will provide a blueprint for a national strategy to prevent scams.

A few highlights from that report include a call for bold government leadership, which includes naming scams as a national priority, asking congressional leadership to mount a coordinated response, and empowering leaders within government to marshal our resources toward a coordinated response.

It will also require driving better law enforcement and intelligence outcomes by providing top officials with clear anti-scam goals and sufficient funding. We must enhance their powers to prosecute while upgrading their capabilities. Criminals are using the most sophisticated technologies, and so must we.

Of course, the private sector has a role to play as well. Specific actions related to the private sector in the report will include things like enacting robust anti-scam policies, strengthening system defenses around the better vetting of platform users, investing in cross-sector information exchanges, and improving the effectiveness of just-in-time warnings and interventions.

In closing, I want to tell you how inspired I have been over the last year by leaders in government and the private sector who are committed to taking serious action.

The American public is asking all of us to take this seriously. Bipartisan majorities of U.S. adults say the Federal Government is doing a bad job of handling online scam attacks and there is lots of upside to working on this, not the least of which is returning \$158 billion a year to our economy.

Thank you.

[The prepared statement of Ms. Griffin follows:]

Testimony for the Record
Submitted to the House Committee on Financial Services
Subcommittee on Oversight and Investigations
Hearing on “Fraud in Focus: Exposing Financial Threats to American Families”
September 18, 2025

Kate Griffin
Director, National Task Force on Fraud and Scam Prevention
The Aspen Institute Financial Security Program

Chairman Meuser, Ranking Member Green, and distinguished members of the Subcommittee,

Thank you for inviting me to testify today on an issue that is presenting a threat to our national security, to the systems of communication, commerce, and finance in our country, and to Americans’ household financial security: Scams - the ability of criminals to deploy sophisticated technological tools and psychological warfare to socially engineer everyday consumers into sending money and personal information.

The United States is caught in a global conflict with these scammers and we are not yet winning. Working mostly from safe havens overseas, criminals are exploiting America’s communications, banking, and digital platforms to deceive Americans into sending money, divulging sensitive information, or worse. A majority of Americans say they get scam calls, emails, and texts at least weekly, and more than 50 million U.S. adults have lost money to an online scam or attack. This causes American households to lose more than two billion dollars *every week*, among other harms. Often, scammers are part of transnational criminal organizations that use fraud and scams to fund other crimes, including drug and human trafficking. In addition to lowering criminals’ barriers to entry, cryptocurrency and artificial intelligence-powered deepfakes are fueling the scams boom, enabling ever-faster and more powerful forms of criminal deceit.

Over the last year, the Aspen Institute Financial Security Program (Aspen FSP) has convened the **National Task Force for Fraud and Scam Prevention** to bring together parties with an interest in stopping this crime, protecting consumers, and restoring trust in our systems. During that time, at least 300 experts from more than 80 organizations – including some of the largest companies on the frontlines against scammers, such as JPMorgan Chase, Google, Target, Microsoft, Verizon, Amazon, and Meta – contributed thousands of hours to it.¹ It is the first time such a broad collection of leaders from

government, law enforcement, private industry, and civil society have come together in the United States to help develop a strategy aimed at preventing fraud and scams.

My testimony today reflects the insights gained from the Task Force and summarizes key recommendations from Aspen FSP based on this experience, which we will soon publish in a major new report. We believe that America can fix the scam problem by deploying the best of the American spirit: bold leadership, innovative thinking, and well-coordinated effort.

Overview of the Scams Threat

Scams are a whole-of-society threat to America

- 1 in 5 U.S. adults (53 million) claim they lost money to an online scam or attack.ⁱⁱ
- Among victims who lost money to scams or online attacks, three-quarters have never filed reports with law enforcement.ⁱⁱⁱ Victims cite confusing procedures, shame, and hopelessness as reasons for not seeking help from authorities.^{iv}
- Still, FBI and FTC complaints document about \$16 billion and \$12 billion in annual losses, respectively, and the FTC estimates that actual fraud-related losses to U.S. consumers, accounting for under-reporting, exceed \$158 billion per year.^v
- Bipartisan majorities of U.S. adults say the federal government is doing a “bad job” handling online scams and attacks.^{vi}
- Research suggests that the scams industry now rivals the size of the illicit drug trade and is growing fast.^{vii} Scam losses reported to law enforcement have more than tripled since 2019.^{viii}
- Everyone is at risk of becoming a scam victim.^{ix} Younger adults report experiencing scams in their households more than older adults, while older adults report losing about twice as much money when they are scammed.^x

Text, phone, email, social media, and financial systems in America are at risk

- Most U.S. adults report receiving scam messages daily or weekly through phone (68%), email (63%), or text (61%) and 33% report the same through social media.^{xi}

- 6 in 10 Americans or more say online scams are a “major problem” on text and phone, email, and social media, while roughly half say the same about shopping, banking, and payment sites or apps.^{xii}
- Being tricked by a scammer to send money or provide access to a financial account is the second-largest crime concern in the U.S. (57% of adults worry about it).^{xiii}
- Victims rarely report financial fraud to law enforcement: Most victims (7 in 10) reported directly to their financial institutions, while only 1 in 10 reported to local law enforcement and 1 in 17 reported to a federal agency.^{xiv}

Scams are a national security threat and a national priority

- The Annual Threat Assessment of the U.S. Intelligence Community has identified scams as part of a nexus of “criminal activity threatening the United States” perpetrated by Transnational Criminal Organizations (TCOs) and state-affiliated groups that also engage in human trafficking, drug trafficking, and weapons and human smuggling.^{xv} But to date, officials have not designated scams against American households as a discreet threat or target for disruption.
- North Korean hackers, Mexican cartels, Russian crime syndicates, and Triad gangs are among the U.S. adversaries that benefit from scams and other financial crimes.^{xvi}
- U.S. Department of the Treasury’s Office of Foreign Assets Control has imposed sanctions state & non-state sponsored TCOs for scam related activity, including Southeast Asian Networks operating in Shwe Kokko, Burma, a notorious hub for virtual currency investment scams under the operational control of the OFAC-designated Karen National Army (KNA)^{xvii}, The Zhao Wei Transnational Criminal Organization operating in the illusive scam compound at the border of Myanmar, Laos, and Thailand, also known as The Golden Triangle Special Economic Zone^{xviii}, and The Lazarus Group, which has ties to the North Korean government, channels revenues generated from fraud and scams to the regime^{xix}. The FBI has issued warnings about The Jalisco New Generation Cartel running scam call centers that finance narcotics trafficking and money laundering.^{xx}

More information on scam trends can be found in the appendix.

Transnational Scams Require a Paradigm Shift for Law Enforcement and Intelligence

The escalating threat of transnational criminal organizations (TCOs) operating overseas while interacting digitally with millions of U.S. consumers fundamentally redefines criminal behavior. This demands a paradigm shift in the national response.

Traditional civil law enforcement tactics, such as domestic lawsuits and domestic asset freezing, often have little deterrence effect against such overseas criminals. Similarly, domestic criminal law enforcement approaches, traditionally focused on post-facto investigation and prosecution, can be overwhelmed by the challenge of protecting people and property against the high-tech, high-speed, high-volume global threat that scammers represent.

To counter this challenge effectively, government responses must evolve. Increasing the nation's capability to stop scams before they happen requires policies that drive a pivot toward preventing financial crime. Law enforcement agencies will have to become more focused on disrupting scam criminals. The U.S. Intelligence Community will have to prioritize detecting transnational scam activity and working to protect Americans from it. All agencies will have to become more coordinated and share more actionable scam intelligence with each other and with companies; and they will have to increase their capacity to analyze information and act on it to effectively counter the speed and technical sophistication of transnational scam criminals.

A Call to Respond

Companies and government agencies are expending extraordinary effort to fight scams against consumers. They have had some success, and the recommendations in the forthcoming report reflect lessons they have learned. But more is needed. The scams threat continues to grow as large volumes of criminals use rapidly evolving tactics to challenge the limits of our systems.

A **whole-of-ecosystem** response is urgently needed to undermine the criminal scam business model, strengthen systems, and protect consumers.

The national response must emphasize government and private sector collaboration.

- **Corporate leaders** must act decisively to suppress scam activity at every stage of its lifecycle. They must empower staff with resources and guidance to maintain robust anti-scam policies and respond effectively when scams occur.

- **Policymakers** must act boldly to enable the required response. **Congress** and the **White House** should recognize scams as a national security threat and priority. They must empower a comprehensive private sector response by enhancing incentives and modernizing legal frameworks; and they must drive better law enforcement and intelligence outcomes by tasking top officials with clear anti-scam goals, backed by sufficient funding and cross-jurisdictional authority.

Corporate Recommendations

Companies in sectors targeted or exploited by scammers, including telecommunications, messaging, digital platforms (social media, paid advertising, and retail), and financial services (banking, fintech, payments, and crypto) should:

- **Maintain robust anti-scam policies addressing the entire scam lifecycle.** C-suite level leaders should own these policies and include accountability mechanisms, adequate budget allocations, and clear expectations for customer service and data protection.
- **Strengthen system defenses.** Improve identity verification and authentication to block inauthentic actors, including evaluating the trustworthiness of advertisers and merchants. Use technology such as liveness testing and interoperable digital credentials to disrupt non-authentic communications.
- **Enhance capabilities to detect suspicious activity.** Invest in private information exchanges with companies in other sectors. Help improve standards for interoperability and ethical governance. Direct legal counsel to establish suitable compliance policies or seek necessary regulatory guidance or safe harbors.
- **Disrupt scams in process.** Take reasonable steps against suspicious activity based on actionable scam intelligence. Take down fraudulent communications channels (e.g. websites), deactivate accounts and profiles of bad actors, and dismantle scammer infrastructure. Continuously improve just-in-time warnings and interventions for customers.
- **Improve reporting and recovery mechanisms.** Share more actionable scam intelligence with law enforcement agencies. Promote effective recovery for victims by providing user-friendly reporting and dispute resolution mechanisms and ensuring fast correction of false positives or account takeovers (ATO).
- **Measure and evaluate interventions.** Pilot the proposed metrics framework for scams and report on results.^{xxi}
- **Collaborate with peers to strengthen scam defenses.** Share best practices across relevant industry sectors and advocate for policy improvements.

Public Policy and Government

The federal government and law enforcement and intelligence agencies, alongside state counterparts, should:

- **Elevate scam prevention as a national priority.** Starting with the White House and Congress, recognize scams as a national security threat and make scam prevention a whole-of-government priority. Establish a national strategy to combat scams, with dedicated resources and broad coordination mechanisms, such as a Congressional Commission or an administrative czar or division with whole-of-government authority. Empower and direct law enforcement and intelligence agencies to improve scam prevention outcomes.
- **Enhance incentives and modernize legal frameworks for combating scams.** Clarify duties for companies to prevent scam activity and de-risk participation in scam suppression efforts, by enacting “good Samaritan” liability protections for companies acting reasonably and in good faith.
- **Enhance law enforcement capabilities.** Increase statutory powers for asset seizure and recovery across all forms of money movement (including digital assets) and punishing transnational illicit financial activity. Create specialist anti-scam units, allocate resources, and develop training programs to improve recognition of scam activity and respond to it.
- **Combat cross-border financial crime.** Apply sanctions and use diplomatic tools against foreign governments and private parties that enable or benefit from scams. Formalize diplomatic engagements with allied nations to shut down scam centers. Improve intelligence gathering to disrupt transnational scam activity.
- **Modernize data collection and analysis.** Review and upgrade key law enforcement databases to improve data intake, analysis, and interoperability, leveraging modern technology like APIs and artificial intelligence (starting with FBI’s Internet Crime Complaint Center (IC3), FTC Sentinel, and FinCEN’s Suspicious Activity Reports (SARs) systems). Create a single portal (e.g. stopscams.gov) for companies to report scam intelligence, including mechanically or in bulk, with the system distributing inputs to the appropriate government databases. Enhance law enforcement analytical capabilities to identify trends and improve deconfliction across agencies.
- **Improve feedback loops.** Law enforcement agencies should publish regular analysis of scam trends and prosecutions to industry and the public.
- **Implement recommendations from the U.S. Government Accountability Office (GAO).** Standardize measurement across agencies and develop a single,

government-wide estimate of affected consumers and dollar losses, factoring in underreporting.^{xviii}

Reforms Specific to Financial Services Policy

As part of a national strategy to combat scams, Aspen FSP's upcoming report will detail several reforms specifically relating to financial services, including:

- **Enhance information sharing efforts** to improve availability of actionable scam intelligence, by re-architecting the FinCEN SARS database to enable higher-volume and more automated data exchange and improving linkages with similarly revitalized FBI IC3 and FTC Sentinel databases.
- **Clarify or expand legal safe harbors** enabling financial institutions and non-financial institutions to exchange actionable scam intelligence and collaborate to prevent scams.
- **Establish parity of law enforcement powers across money movement**, including civil forfeiture of digital assets.
- **Enable risk-based payment pauses / limits** and other reasonable interventions to disrupt suspected malicious interactions.
- **Pilot bank-to-law enforcement victim report sharing.** Research shows that the vast majority of scam victims report the problem to their bank, while only a small portion report directly to a local or federal law enforcement agency.

Across the Ecosystem

All stakeholders should take a risk-based approach to flexibly prioritize interventions against the most impactful, and evolving, scam activities. Broader initiatives and cross-sector efforts should include:

- **Foster offensive technological innovation.** Use of artificial intelligence and advanced analytics is likely to be crucial for enhancing private and public sector capabilities in scam detection, prevention, and response.
- **Strengthen public awareness and consumer empowerment.** Study and improve consumer education, warning, and intervention practices. Increase funding for targeted, coordinated public awareness campaigns to help consumers recognize scams, reduce the stigma of victimization, and drive useful action such as reporting scams to a national law enforcement portal.
- **Assess potential benefits of establishing a U.S. National Anti-Scam Center.** Commission a study to determine the merits of creating a national hub that combines a reporting portal with professional training, public awareness, and victim support resources. A useful example of something similar is the National

Center for Missing and Exploited Children (NCMEC), a private non-profit organization established by President Ronald Reagan.

These and other recommendations are further explained in Aspen FSP's soon-to-be published report, a preview of which is attached to this letter as an appendix. The report is titled "United We Stand: A National Strategy to Prevent Scams. " It presents recommendations for government and private sector collaboration to combat fraud against consumers, cut off criminal funding, and protect the United States. Aspen FSP will publish the report in early October of this year. We would be happy to brief Committee members and staff upon its release.

Appendix: Understanding Scam Trends

We are seeing increased, record-breaking losses to fraud and scams across the board

- Last year, the FBI received over 850,000 fraud and cybercrime complaints, with losses hitting a record \$16.6 billion, a 33% increase over 2023.^{xxiii}
- The biggest financial toll came from investment scams, at over \$6.5 billion. This was followed by business email compromise at \$2.77 billion and tech support fraud at \$1.46 billion.^{xxiv}
- The most common scam types were phishing, spoofing, extortion, and personal data breaches.^{xxv}

Older Americans are continuing to bear the financial greater financial cost of fraud and scams while younger Americans experience them more frequently

- In 2024, Americans aged 60+ filed 147,000 complaints with the FBI, the highest of any age group, and suffered \$4.9 billion in losses—with an average loss of \$83,000.^{xxvi}
- The FBI notes that over 33,000 seniors were targeted through crypto scams on phones and apps, leading to \$2.8 billion in losses.^{xxvii}
- People aged 70+ file half as many reports with losses compared to young adults, but their total losses are nearly 1.5 times greater than those of young people.^{xxviii}

Call center, imposter, and AI-generated scams are scaling fast

- Call center scams—especially targeting seniors—remain one of the most lucrative and destructive tactics. In 2024, call center scams led to \$1.9 billion in losses, often through impersonation of tech support or government agencies.^{xxix}
- The FTC also reported that imposter scams, including romance, tech support, and government impersonation, led to \$2.95 billion in losses, with a median loss of \$800.^{xxx}
- The FBI warned that criminals are increasingly exploiting artificial intelligence to create more convincing scams with less effort, using AI-generated images, audio, and video to impersonate trusted sources and deceive victims at scale.^{xxxi}

Appendix: Preview of Forthcoming Report

“United We Stand: A National Strategy to Prevent Scams” (Preview)

The following is a preview of recommendations that Aspen FSP will publish in early October, 2025. The report presents recommendations for government and private sector collaboration to combat fraud against consumers, cut off criminal funding, and protect the United States.

Part One of the report is tactical, suggesting company and government agency actions to suppress scam activity and respond to it, at each stage of the fraud lifecycle. Part Two is structural, suggesting public policy and corporate practice reforms to empower scam prevention efforts. Each recommendation will offer one or more principles to guide action, paired with a set of “practical next steps and possible solutions” to give practitioners concrete ideas to test or implement.

Below is the report’s Table of Contents for reference.

PART ONE: ACT AGAINST SCAMS AND MINIMIZE THEIR HARM

A. SUPPRESS SCAM ACTIVITY

- 1) Deter criminals from engaging in scam activity
 - a) Invest in deterring cross-border financial crime as applied to scams
 - b) Enhance domestic law enforcement powers and resources
- 2) Defend systems against inauthentic communications
 - a) Maintain strong corporate anti-scam policies
 - b) Improve credentialing of users and businesses that could be scammers
 - c) Make it harder for scammers to communicate with victims
 - d) Reduce barriers to flagging suspicious users/activity
- 3) Detect inauthentic or criminal activity on targeted platforms
 - a) Invest in scam detection
 - b) Align information sharing priorities
 - c) Address real and perceived barriers to information sharing
 - d) Improve interoperability of private sector and law enforcement databases
- 4) Disrupt scams in process
 - a) Clarify policies for expeditious takedown of fraudulent accounts
 - b) Leverage and invest resources in take-down services
 - c) Improve just-in-time warnings and interventions

B. RESPOND TO SCAM ACTIVITY

- 1) Revitalize law enforcement reporting practices

- a) Improve law enforcement's ability to consume scam-related data in bulk, starting with three key databases
 - b) Create a simple mechanism to report bulk information to law enforcement
 - c) Improve law enforcement feedback loops to industry and the public
 - 2) Improve consumer reporting mechanisms
 - a) Simplify and standardize consumer reporting channels
 - b) Create feedback loops for consumers
 - c) Establish mechanisms to share victim reports with law enforcement
 - 3) Promote effective scam recovery
 - a) Address false positives that arise from prevention efforts
 - b) Maintain effective methods to correct account takeover problems
 - c) Promote victim support services
 - 4) Measure scam activity and evaluate interventions
 - a) Advance the field of fraud and scam measurement
 - b) Measure the effectiveness of interventions
 - c) Implement GAO recommendations to improve government scam metrics
- PART TWO: EMPOWER SCAM PREVENTION EFFORTS**
- A. ELEVATE GOVERNMENT LEADERSHIP AND CAPABILITY**
 - 1) Establish scam prevention as a national priority and budget for it
 - a) Announce scam prevention as a national priority or security threat
 - b) Formalize a national strategy to combat scam activity
 - 2) Modernize government's data analysis capabilities for fighting financial crimes
 - B. ENHANCE INCENTIVES & MODERNIZE THE LEGAL FRAMEWORK FOR COMBATING SCAMS**
 - C. ELEVATE CORPORATE ANTI-SCAM POLICIES AND LEADERSHIP**
 - 1) Maintain robust corporate anti-scam policies and governance
 - 2) Work with peer organizations to drive whole-of-ecosystem improvement
 - D. INVEST IN PUBLIC AWARENESS AND RESOURCES**
 - 1) Evaluate and improve consumer education practices
 - 2) Increase coordination and efficacy of public awareness campaigns
 - E. ASSESS POTENTIAL BENEFITS OF A U.S. NATIONAL ANTI-SCAM CENTER**

Endnotes

- ⁱ To see a full list of member institutions, visit <https://fraudtaskforce.aspeninstitute.org/membership>
- ⁱⁱ Jeffrey Gottfried, Eugenie Park, and Monica Anderson, "Online Scams and Attacks in America Today." Pew Research Center, July 31, 2025. <https://www.pewresearch.org/internet/2025/07/31/online-scams-and-attacks-in-america-today/>. A ratio of 1 in 5 adults equates to approximately 53 million adults, based on a total U.S. adult population of approximately 267 million. See: U.S. Census Bureau, "National Population by Characteristics: 2020-2024," June 2025. <https://www.census.gov/data/tables/time-series/demo/popest/2020s-national-detail.html>.
- ⁱⁱⁱ Gottfried, Park, and Anderson, "Online Scams and Attacks in America Today."
- ^{iv} Many fraud victims do not report their crimes due to feelings of shame, guilt, or embarrassment, doubts about their own judgment, fear of others' reactions, or belief that their losses are too small or that law enforcement will not act. Victims often blame themselves, even though skilled perpetrators are responsible. See, e.g., U.S. Department of Justice, Western District of Washington. "Financial Fraud Crime Victims." Last modified January 30, 2025. <https://www.justice.gov/usao-wdwa/victim-witness/victim-info/financial-fraud>. Victim-blaming culture aimed at financial fraud victims, exacerbates victims' deep sense of shame and low self-esteem and shifts the focus away from perpetrators. See, e.g., AARP Fraud Watch Network and FINRA Investor Education Foundation, in collaboration with Heart + Mind Strategies. "Blame and Shame in the Context of Financial Fraud: A Movement to Change Our Societal Response to a Rampant and Growing Crime." June 2022. <https://www.finrafoundation.org/sites/finrafoundation/files/Blame-and-Shame-in-the-Context-of-Financial-Fraud.pdf>.
- ^v The 2024 Internet Crime Report combines information from 859,532 complaints of suspected internet crime and details reported losses exceeding \$16 billion—a 33% increase in losses from 2023. See: Federal Bureau of Investigation. "Internet Crime Report 2024." Internet Crime Complaint Center (IC3). April 24, 2025. <https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report>. Of the 2.6 million fraud reports, 38% indicated money was lost. In 2024, people reported losing over \$12 billion to fraud—an increase of over \$2 billion over 2023. See: Federal Trade Commission. "Sentinel Network Data Book 2024." March 2025. <https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2024>.
- ^{vi} Gottfried, Park, and Anderson, "Online Scams and Attacks in America Today."
- ^{vii} The rise of online scams represents a substantial transfer of wealth from middle-class households to organized criminal networks. See, e.g., The Economist. "Online Scams May Already Be as Big a Scourge as Illegal Drugs." February 6, 2025. <https://www.economist.com/briefing/2025/02/06/online-scams-may-already-be-as-big-a-scourge-as-illegal-drugs>.
- ^{viii} Reported scams in the U.S. rose between 2020 and 2024, with consumer complaints increasing from 4.7 million to 6.5 million and fraud losses growing from \$3.3 billion to \$12.5 billion (see, e.g., Federal Trade Commission 2020; 2024). U.S. Federal Trade Commission. "Consumer Sentinel Network Data Book 2020." Federal Trade Commission. https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf. U.S. Federal Trade Commission. "Consumer Sentinel Network Data Book 2024." Federal Trade Commission. https://www.ftc.gov/system/files/ftc_gov/pdf/csn-annual-data-book-2024.pdf.
- ^{ix} National Consumers League. "Top Ten Scams of 2024." January 16, 2025. <https://nclinet.org/wp-content/uploads/2025/01/Top-Scams-of-2024.pdf>.
- ^x Younger households report experiencing scams at higher rates compared to older adults. According to a Gallup poll conducted in 2023, 22% of adults under 30 reported that someone in their household had fallen victim to a scam in the past year. This is notably higher than the 9% reported by those aged 50–64 and the 13% by those aged 65 and older. See, e.g., Gallup. "Scams Relatively Common, Anxiety-Inducing for Americans." July 31, 2023. <https://news.gallup.com/poll/544643/scams-relatively-common-anxiety-inducing-americans.aspx>. Seniors reported \$1.18 billion in fraud losses, compared to \$810 million reported by adults in their 30s. Despite the higher financial losses among seniors, the number of fraud reports from both age groups was similar, indicating that seniors are losing approximately 50% more per incident than their younger counterparts.

See, e.g., U.S. Federal Trade Commission. "Consumer Sentinel Network Data Book 2024."

^{xi} Gottfried, Park, and Anderson, "Online Scams and Attacks in America Today."

^{xii} Ibid.

^{xiii} Gallup. "Scams: Relatively Common and Anxiety-Inducing for Americans."

^{xiv} Fulford, Scott. "More Than a Quarter of Americans Lost Money to Financial Fraud." *LinkedIn*, August 2025. <https://www.linkedin.com/pulse/more-than-quarter-americans-lost-money-financial-fraud-scott-fulford-2qije>. Estimates were calculated using the publicly accessible CFPB 2024 Making Ends Meet Survey data: <https://www.consumerfinance.gov/data-research/making-ends-meet-survey-data/>.

^{xv} Office of the Director of National Intelligence. "Annual Threat Assessment of the U.S. Intelligence Community." March 2025. <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf>.

^{xvi} TRM Labs. "All Roads Lead to China: North Korean Hackers, Fentanyl, Cartel Money Laundering, and Global Organized Crime." May 27, 2025. <https://www.trmlabs.com/resources/reports/all-roads-lead-to-china>. See also: Ken Westbrook, "As Scams by Foreign Organized Crime Soar, Here's How America Must Respond" (Stop Scams Alliance, December 2024), accessed September 3, 2025, PDF, 4-5.

^{xvii} "Treasury Sanctions Southeast Asian Networks Targeting Americans with Cyber Scams" U.S. Department of the Treasury press release, September 8, 2025. <https://home.treasury.gov/news/press-releases/sb0237>

^{xviii} "Treasury Sanctions the Zhao Wei Transnational Criminal Organization" U.S. Department of the Treasury press release, January 30, 2018. <https://home.treasury.gov/news/press-releases/sm0272>

^{xix} "Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups" U.S. Department of the Treasury press release, September 13, 2019. <https://home.treasury.gov/news/press-releases/sm774>

^{xx} "Mexican Cartels Target Americans in Timeshare Fraud Scams, FBI Warns" FBI News Story, June 7, 2024. <https://www.fbi.gov/news/stories/mexican-cartels-targeting-americans-in-timeshare-fraud-scams-fbi-warns>

^{xxi} "Fraud and Scam Measurement Framework". Aspen Institute National Task Force on Fraud and Scam Prevention. https://static1.squarespace.com/static/671a80aa4a84f2359ce4d360/t/6830b13e294cb446da01973d/1748021566525/MeasurementFramework_5-23-25.pdf

^{xxii} "Consumer Protection: Actions Needed to Improve Complaint Reporting, Consumer Education, and Federal Coordination to Counter Scams" Government Accountability Office, April 8, 2025. <https://www.gao.gov/products/gao-25-107088>

^{xxiii} FBI, 2024 Internet Crime Report, p. 4.

^{xxiv} Ibid, p. 10

^{xxv} Ibid, p. 9

^{xxvi} Ibid, p. 27

^{xxvii} FBI, 2024 Internet Crime Report, p. 35.

^{xxviii} FTC, Consumer Sentinel Network Data Book 2024, p. 6.

^{xxix} FBI, 2024 Internet Crime Report, pp. 11, 14.

^{xxx} FTC, Consumer Sentinel Network Data Book 2024, p. 8.

^{xxxi} FBI Alert Number: I-120324-PSA, 2024

Chairman MEUSER. Thank you very, very much. We look forward to your report.

Ms. Sanchez-Adams, you are now recognized for 5 minutes.

**STATEMENT OF CARLA SANCHEZ-ADAMS, SENIOR ATTORNEY,
NATIONAL CONSUMER LAW CENTER**

Ms. SANCHEZ-ADAMS. Chairman Meuser, Ranking Member Green, members of the committee, thank you for the opportunity to testify on behalf of the National Consumer Law Center's low-income clients.

Payment fraud is a national crisis demanding a national, holistic response from our government. Payment fraud impacts all Americans regardless of age, race, education, income, or political affiliation.

Now, technology has enabled criminal fraudsters to use older forms of payment—like bank-to-bank wire transfers and checks—to steal money, and these lack sufficient protections. Newer forms of payment, such as peer-to-peer transactions and crypto transfers, also enable criminals to steal and launder money in an easier form.

Payment fraud can be sorted into two buckets: unauthorized and fraudulently induced.

Unauthorized transactions occur when a criminal fraudster initiates a transaction on behalf of the victim but without their knowledge or permission.

On the other hand, fraudulently induced transactions occur when the consumer or the victim themselves initiates the transaction but only as a result of a fraud scheme using deception or manipulation.

Now, as you have heard, criminal fraudsters, they spoof real numbers of financial institutions via text message or phone call. They use deepfakes, take over accounts through malware or breaches, resort to manipulative psychological practices, and even use violence to get victims to initiate payments.

Americans are plagued by both types of fraud, and we need to address both if we are going to combat fraud and instill confidence in our banking and payment systems but the responses that fraud victims get vary greatly depending on the payment method used. A victim's best chance at getting their money back is if there was an unauthorized breach of their accounts because of the strong protections of the Electronic Fund Transfer Act, or EFTA.

But EFTA's Regulation E exempts certain wire transfers, leaving victims with weak State laws, while electronic benefit transfer (EBT) cards are unprotected entirely and if the transaction was fraudulently induced, which you all call a scam, then usually the victim is going to hear, "Sorry, there is nothing we can do," because there are no clear protections under the law.

We therefore need to update antiquated laws that offer little to no protection to victims impacted by fraud. In this day and age, where the vast majority of transactions occur online or through a mobile app, it makes no sense that only some of these transactions are covered by EFTA and not others.

We also need to update EFTA to include fraudulently induced transfers, following the example of the U.K., which recently adopted rules reimbursing victims of authorized push-payment fraud,

with industry recognition that making consumers safe is central to confidence in the payment systems.

Protecting victims should be central to any discussion about combating fraud. We absolutely cannot push the burden of fraud entirely onto its victims. Consumer education is important and necessary, but it alone will not solve the problem of fraud, especially with fraud schemes and technology that are ever evolving.

However, there are steps that we can collectively take to keep the impacts of fraud on innocent consumers and even financial institutions to a minimum and to incentivize more effective use of innovation to prevent fraud and make our system safe.

I agree that telecommunication and social media companies must take action to prevent fraud in the first instance, especially since some know that they are carrying fraudulent traffic. If a criminal fraudster cannot contact a victim through fake texts, spam calls, or social media schemes, then the fraud cannot occur.

Payment systems and financial institutions must also bear greater responsibility in the fight against fraud. Criminal fraudsters need a way to receive those stolen funds. If these criminals cannot get access to our payment rails or deposit holding accounts, then innocent victims will not lose money that way.

As such, we need a stronger focus on the know-your-customer obligations of the financial institution or payment provider that allowed the fraudster or money mule to open an account and receive the fraudulent funds.

Victims should be reimbursed by the banks, who, in turn, should be reimbursed by the institution that received the fraudulent payment. If they bear liability, they will use more innovative technology to detect and stop fraud. This already happens on certain payment networks when there are claims of unauthorized use.

Simultaneously, we must give innocent consumers the right to a swift resolution if their funds are frozen or closed by overly aggressive fraud reporting.

This is not the time to be weakening consumer protection or the agencies that protect consumers. This CFPB was actively working on addressing fraud but is now in tatters and Congress blocked the CFPB from supervising peer-to-peer (P2P) apps, which would have helped fraud victims and with the change in leadership, the CFPB dismissed an enforcement action involving fraud on Zelle.

Meanwhile, President Trump has sparked an effort to reduce the number of checks sent through the mail to and from the government, which is incredibly important given the rash of check washing fraud, but people will not be comfortable making or receiving electronic payments if fraud is rampant.

Moreover, we should not encourage the use of stablecoins, crypto assets, and the crypto exchanges when they are a vector for fraud and scams. These payment forms and systems cannot be outside of our consumer protection laws.

Thank you, and I am happy to take any questions.

[The prepared statement of Ms. Sanchez-Adams follows:]

“Fraud in Focus: Exposing Financial Threats to American Families”

**Oversight and Investigations Subcommittee of the U.S. House Financial
Services Committee**

Thursday, September 18, 2025

Testimony of Carla Sanchez-Adams

**National Consumer Law Center
on behalf of its low-income clients**



“Fraud in Focus: Exposing Financial Threats to American Families”

**Oversight and Investigations Subcommittee of the U.S. House
Financial Services Committee**

Testimony of Carla Sanchez-Adams
Thursday, September 18, 2025

Executive Summary	2
I. Fraud Is a National Threat That Affects Everyone.	5
II. Payment Systems and Telecommunication and Social Media Companies Play an Important Role in Enabling or Preventing Fraud and in Protecting Consumers.	6
III. Person-to-Person (P2P) Payment Fraud.	7
A. The prevalence of P2P use and the incidence of fraud on these platforms.	7
B. How technology perpetuates P2P fraud and theft.	9
C. Current ambiguity in the law leaves consumers insufficiently protected from P2P fraud.	10
D. Responsibility of receiving institutions.	11
E. Problems with P2P apps when consumers make mistakes.	12
F. Potential remedies to address P2P payment fraud.	13
1. Update the Electronic Funds Transfer Act.	13
2. Consider the United Kingdom as an example.	13
3. When liability is split between sending and receiving institutions and not pushed onto consumers, more will be done to protect consumers.	15
4. Address the lack of oversight for certain parties involved in the payments market.	17
IV. Fraud through Crypto-Assets.	17
A. Crypto-assets are a common payment method for criminal fraudsters.	17
B. Crypto companies must be subject to the same BSA requirements as banks.	18
C. Stablecoins and crypto-assets must be subject to consumer protection statutes such as the EFTA when used for consumer payments.	20
V. Bank-to-Bank Wire Transfer Fraud.	20
A. Consumers are devastated by bank-to-bank wire transfer fraud.	20
B. Technology enables more bank-to-bank wire transfer fraud.	24
C. Banks claim bank-to-bank wire transfers are exempt from the EFTA, leaving consumers exposed to losing thousands of dollars.	24
D. Potential remedies to address bank-to-bank wire fraud.	26

VI. Check Fraud.	27
A. Check alteration fraud is on the rise.	27
B. Though some protections exist for consumers harmed by check fraud, they are often left scrambling.	28
C. Potential remedies to address check fraud.	29
VII. Electronic Benefit Transfer (EBT) Card Fraud.	30
A. EBT card skimming and theft leave cardholders without any protections.	30
B. Potential remedy to address EBT card fraud.	31
VIII. Problems with the Collection of Accurate Payment Fraud Data Create an Additional Barrier to Addressing Payment Fraud.	32
A. The problem of fragmented data collection on payment fraud.	32
B. Potential remedies to address the problem of fragmented payment fraud data collection.	33
1. Interagency collaboration.	33
2. Simplify fraud reporting.	34
3. Require fraud reporting within payment systems.	35
4. Require FinCEN to update the Suspicious Activity Report (SAR) to capture information about accounts that receive fraudulent funds.	35
5. Ensure consumers are protected from false positives.	36
IX. Challenges with Account Freezes, Closures, and Holds Due to Fraud Lead to Debanking Consumers.	37
A. Overaggressive fraud algorithms can shut out innocent consumers from access to their bank accounts and funds, and overly broad BSA programs prevent these consumers from understanding why those actions were taken.	38
B. Potential remedies to address improper freezes or account closures due to the use of automated fraud detection.	40
X. Fraud Traverses Many Industries and Sectors, and the Federal Government Must Take a Holistic Approach to Combatting Fraud.	40
A. Criminal Fraudsters rely heavily on text messages to initiate fraud schemes.	40
B. Recommendations to address scams initiated by text.	41
XI. Fraud Prevention Education Is Necessary in the Fight Against Fraud, But It Will Not Solve the Problem.	43
XII. Conclusion	45

Chairman Meuser, Vice Chairman Moore, Ranking Member Green, and Members of the Subcommittee, thank you for inviting me to testify today regarding fraud and its impact on American families. I am Carla Sanchez-Adams, a senior attorney at the National Consumer Law Center. I offer my testimony on behalf of NCLC's low-income clients.

Since 1969, the nonprofit National Consumer Law Center® (NCLC®) has used its expertise in consumer law to work for consumer justice and economic security for low-income and vulnerable consumers in the United States. NCLC's expertise includes policy analysis and advocacy; consumer law and energy publications; litigation; expert witness services; and training and advice for advocates. NCLC works with nonprofit and legal services organizations, private attorneys, policymakers, and federal and state government and courts across the nation to stop exploitative practices, help financially stressed families build and retain wealth, and advance economic fairness. NCLC has long advocated for stronger laws, regulations, and enforcement to ensure that consumers' funds and payments are safe and to prevent and remedy fraud.

I am one of the co-authors of NCLC's treatise, *Consumer Banking and Payments Law*. My colleagues and I interact with legal services, government, and private attorneys, as well as community groups and organizations from all over the country who represent low-income and vulnerable individuals on consumer issues. As a result of our daily contact with these advocates, we have seen many examples of the damage wrought by payment fraud from every part of the nation. It is from this vantage point that I supply this testimony.

NCLC has previously provided testimony before Congress on the need to address payment fraud.¹ Additionally, NCLC has provided feedback to various regulatory agencies on the same issue.² I reiterate and incorporate those comments here as well.

¹ See Testimony of Carla Sanchez-Adams, NCLC "Examining Scams and Fraud in the Banking System and Their Impact on Consumers," Hearing Before the U.S. Senate Committee on Banking, Housing, and Urban Affairs, (February 1, 2024), available at <https://www.nclc.org/wp-content/uploads/2024/02/Written-testimony-The-Problem-of-Payment-Fraud.pdf>; NCLC et al., Statement for the Record, "What's in Your Digital Wallet? A Review of Recent Trends in Mobile Banking and Payments," Hearing Before the House Financial Services Taskforce on Financial Technology at 10-11, (April 28, 2022), available at https://www.nclc.org/wp-content/uploads/2022/10/Digital_Wallet_testimony.pdf; Testimony of Odette Williamson, NCLC "Fraud, Scams and COVID-19: How Con Artists Have Targeted Older Americans During the Pandemic," Hearing Before the U.S. Senate Special Committee on Aging, (September 23, 2021), available at https://www.nclc.org/wp-content/uploads/2022/08/Testimony_Covid_Aging-1.pdf.

² See NCLC, Comments regarding the Request for Information on Potential Actions to Address Payments Fraud by the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, and Federal Deposit Insurance Corporation, (September 15, 2025), available at https://www.nclc.org/wp-content/uploads/2025/09/2025.09.15_Comments_Fraud-RFI-on-Payments-Fraud.pdf; NCLC, Comments regarding the Expansion of Fedwire Funds Service and National Settlement Operating Hours, (September 6, 2024), available at https://www.nclc.org/wp-content/uploads/2024/11/2024.09.06_Comments_NSS-Comments.pdf; NCLC, Comments regarding FinCEN's Rulemaking on Anti-Money Laundering and Countering the Financing of Terrorism Programs, (September 3, 2024), available at https://www.nclc.org/wp-content/uploads/2024/09/2024.09.03_Comments_FinCEN-Dept-Treasury-on-AML-Rulemaking.pdf; NCLC et al., Comments regarding the FTC Collaboration Act of 2021, (August 14, 2023), available at https://www.nclc.org/wp-content/uploads/2023/08/FTC_AG-Fraud-Collaboration-consumer-comments-8-14-23-final3-Lauren-Saunders.pdf; NCLC et al., Letter Urging Federal Reserve Board to Prevent FedNow Errors and Fraud, (August 10, 2022), available at https://www.nclc.org/wp-content/uploads/2022/09/FedNow_fraud_ltr.pdf; Comments of 43 consumer,

Executive Summary

Fraud continues to pose a threat to U.S. households, businesses, financial institutions, and the economy as a whole. In 2024, consumers reported over \$12.5 billion fraud losses to the Federal Trade Commission,³ though total fraud losses are far higher. According to the Pew Research Center, 73% of U.S. adults have experienced some kind of online scam or attack, and one in five U.S. adults reported having lost money because of an online scam or attack.⁴ But the impacts of fraud are most keenly felt by certain vulnerable populations such as older Americans,⁵ communities of color, and low-income consumers,⁶ who have a more difficult time recovering from fraud losses.

Consumers are plagued by problems with unauthorized transactions as well as fraudulently induced payments involving peer-to-peer payment applications, crypto-assets, bank-to-bank wire transfers, check alterations and forgeries, and Electronic Benefits Transfer (EBT) card skimming. The increasing ease and use of mobile and online banking through technological advancement have also simultaneously provided opportunities for scammers to exploit newer payment technologies. However, obtaining a complete and holistic picture of the volume, loss, and threat of payment fraud is difficult because of the fragmented way we collect fraud data.

The financial institutions and companies that design and run these payment systems, including the financial institutions and companies that hold the accounts of criminal fraudsters and money mules that receive fraudulent payments, need to take more responsibility for making these systems safe and protecting consumers. Given the increasing sophistication of fraud schemes, warnings to consumers are insufficient. If payment system participants take responsibility for protecting consumers, they will have the incentive to leverage the latest innovative technologies to prevent and detect fraud and apportion liability among the various system participants, thereby making the entire system safe. At the same time, any attempts to combat fraud must also be tempered with policies and procedures that protect innocent consumers who do not engage in payment fraud but whose funds might be frozen for extended periods of time.

small business, civil rights, community and legal service groups to Federal Reserve Board Re: Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers Through Fedwire, Docket No. R-1750; RIN 7100-AG16, (September 9, 2021), available at <https://bit.ly/FedNowCoalitionComments> ("FedNow Comments").

³ See FTC "New FTC Data Show a Big Jump in Reported Losses to Fraud to \$12.5 Billion in 2024," (Press Release) (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>.

⁴ Anderson, Monica, Gottfried, Jeffrey, and Park, Eugenie, "Online Scams and Attacks in America Today," Pew Research Center, (July 31, 2025), <https://www.pewresearch.org/internet/2025/07/31/online-scams-and-attacks-in-america-today/>. The Pew study found that, "nearly all Americans view online scams and attacks as a national problem. More than nine-in-ten say online scams and attacks are a problem in the country, including 79% who describe them as a major problem. Most U.S. adults have been a victim of an online scam or attack. We find that 73% of U.S. adults have ever experienced things like credit card fraud, ransomware or online shopping scams."

⁵ According to the Federal Trade Commission, though younger people (ages 20-29) reported losing money to fraud more often than older people in 2024, those aged 70+ had a higher median loss than those aged 20-29 (\$1,650 compared to \$417). See

<https://public.tableau.com/app/profile/federal.trade.commission/viz/ConsumerSentinel/Infographic>.

⁶ *Id.* "Black, Hispanic and Asian adults are more likely than White adults to say they have lost money because of an online scam or attack, (and) those with lower incomes (26%) are more likely than those in upper-income households (15%) to say they have lost money in this way. Those in middle-income households fall in between the two other groups (20%)."

Telecommunication companies, including VOIP providers and aggregators, and social media platforms must also take responsibility for keeping criminals off their systems. Most frauds start with a text or a fraudulent social media post on a marketplace or other platform.

To combat payment fraud, we recommend addressing the current gaps and ambiguities in the Electronic Funds Transfer Act (EFTA) that leave consumers unprotected. These include:

- Ensuring consumers are protected from liability when they are defrauded into initiating a transfer;
- Allowing the consumer's financial institution, after crediting the consumer for a fraudulent transfer, to be reimbursed by the financial institution that allowed the criminal fraudster to receive the fraudulent payment;
- Ensuring that the EFTA applies to stablecoins and crypto-assets when used for consumer payments;
- Eliminating the exemptions for bank wire transfers⁷ and electronic transfers authorized by telephone call, bringing those transfers within the EFTA and its protections against unauthorized transfers and errors;
- Eliminating the exclusion of EBT cards from the EFTA, bringing those transfers within the EFTA and its protections against unauthorized transfers and errors;
- Clarifying that the EFTA's error resolution procedures apply when the consumer makes a mistake, such as in amount or recipient;
- Clarifying that the error resolution duties under the EFTA apply if a consumer's account is frozen or closed, or the consumer is otherwise unable to access their funds, with an exception if the consumer was denied access due to a court order or law enforcement, or the consumer obtained the funds through unlawful or fraudulent means; and
- Considering whether consumer protections for checks should be included in the EFTA.

Federal regulators should also take additional steps to address fraud and protect innocent consumers who are harmed by fraud. For example, federal regulators should:

- Enforce and strengthen laws that require financial institutions and other companies to protect consumers from unauthorized and fraudulently induced charges, especially when EFTA violations occur;
- Devote more attention to the responsibilities of institutions that receive fraudulent payments, including stepping up enforcement of Bank Secrecy Act /Anti-Money Laundering obligations;
- Establish interagency collaboration to assist consumers with reporting fraud, collecting data on fraud, and establishing systems for sharing fraud data and findings; and
- Provide guidance to financial institutions about the timelines and procedures for consumers to regain access to improperly frozen funds, including providing clarity about

⁷ As discussed below, Regulation E exempts some wire transfers, though a court has held that that exemption may not apply in every circumstance.

what information can and should be given to accountholders regarding account closures and freezes.

Congress should also pass legislation and work with the Federal Communications Commission (FCC) to address the role that telecommunications providers play in facilitating fraud. Some of these measures include:

- Requiring a bond for transmitters of phone calls and texts.
- Requiring rigorous know-your-customer and know-your-traffic procedures that force carriers to vet callers and calls that transit their network.
- Requiring record-keeping for call originators to ensure that information about callers is available for government or private enforcement efforts.
- Requiring carriers to investigate call traffic that displays suspicious characteristics, like a high percentage of short-duration calls and other indicia of fraud.
- Adopting federal regulations for phone number resellers to address phone number rotation schemes that allow callers to undermine the goals of the STIR/SHAKEN framework.
- Authorizing the FCC to file actions for civil penalties in federal district courts.
- Strengthening the Telephone Consumer Protection Act (TCPA) to encourage robust enforcement against scam callers and those who facilitate fraud.
- Strengthening the Telemarketing Sales Rule (TSR) to expand enforcement.

In the testimony below, I will focus on five payment vehicles that have seen increasing fraud: person-to-person payments, crypto-assets, bank-to-bank wire transfers, check alterations, and Electronic Benefit Transfer cards. I will discuss how these payment frauds impact consumers and how protections can be improved. I will also discuss additional measures needed to combat fraud, such as improving data collection and addressing the problem of false positives when innocent consumers are impacted by account closures or freezes due to fraud.

I. Fraud Is a National Threat That Affects Everyone.

Fraud continues to climb and devastates millions of consumers across the country each year. In 2022, the Federal Trade Commission (FTC) received more than 2.5 million reports of fraud with reported losses totaling almost \$9 billion (\$8,996,000) from its Consumer Sentinel Network.⁸ Those losses were up a shocking 46.7% from 2021. And in just two years (2024), that amount rose to a little over 2.6 million reports of fraud totaling approximately \$12.8 billion in losses, a 42.2% increase in dollars lost.⁹

Additionally, the FTC numbers reflect only fraud cases reported to the Consumer Sentinel Network. Fraud is substantially underreported; only a small percentage of U.S. fraud victims report the fraud to law enforcement.¹⁰

As AARP noted:

“While nearly nine in 10 respondents (87%) feel people should report incidents of fraud, only an estimated 15% contact law enforcement. The gap may be tied to attitudes and awareness about fraud. Sometimes those who have been victimized by a scam feel embarrassed, guilty, or believe there is nothing police can do.”¹¹

Fraud impacts all of us, across every community—the young and the old, those with higher and lower household incomes, as well as the highly educated and those with lower levels of formal education.¹²

While the common belief is that older consumers are more likely to be susceptible, in fact younger people are also significantly likely to experience fraud. But when older people suffer fraud, they lose far more money, as shown by the following FTC chart.¹³

⁸ FTC, *Fraud Reports by Amount Lost*, available at <https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudLosses>.

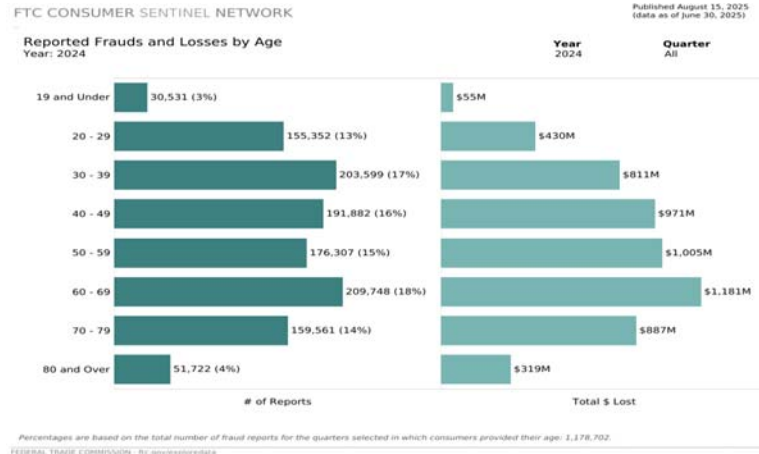
⁹ *Id.*

¹⁰ Anderson, Monica, Gottfried, Jeffrey, and Park, Eugenie, “Online Scams and Attacks in America Today,” Pew Research Center, (July 31, 2025), available at <https://www.pewresearch.org/internet/2025/07/31/online-scams-and-attacks-in-america-today/>. The Pew study found that roughly three-quarters of the survey group did not report to law enforcement that they lost money from an online scam or attack, while only 26% said they had informed law enforcement. See also Department of Justice, U.S. District Attorney’s Office, District of Alaska, *Financial Crime Fraud Victims*, (2020), available at <https://www.justice.gov/usao-ak/financial-fraud-crimes>.

¹¹ Williams, Alicia R., “Americans Are Aware of Fraud’s Pervasiveness but Remain Vulnerable,” AARP Research, (May 17, 2023), available at <https://www.aarp.org/pri/topics/work-finances-retirement/fraud-consumer-protection/fraud-awareness-older-adults/>; see Department of Justice, U.S. District Attorney’s Office, District of Alaska, *Financial Crime Fraud Victims*, (2020), available at <https://www.justice.gov/usao-ak/financial-fraud-crimes>.

¹² Anderson, Monica, Gottfried, Jeffrey, and Park, Eugenie, “Online Scams and Attacks in America Today,” Pew Research Center, (July 31, 2025), available at <https://www.pewresearch.org/internet/2025/07/31/online-scams-and-attacks-in-america-today/>. See also Levinthal, Dave, “Cyberthieves stole \$186,000 from a Republican member of Congress as fraud epidemic plagues political committees,” *Business Insider*, (November 29, 2022), available at <https://www.businessinsider.com/online-fraud-congress-diana-harshbarger-cybertheft-2022-11>.

¹³ FTC, *Reported Fraud and Losses by Age* (2024), available at <https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudLosses>.



Fraud has a particularly harsh impact on low-income families and communities of color, who have fewer resources to help them recover. Fraudsters often take the last dollar from those least able to afford it, and often target older adults, immigrants, and other communities of color.

II. Payment Systems and Telecommunication and Social Media Companies Play an Important Role in Enabling or Preventing Fraud and in Protecting Consumers.

Criminal fraudsters who steal money through fraud schemes need a way to contact a victim to initiate the fraud scheme and a way to obtain a victim's money. They use a variety of avenues to contact their victims, including text messages, phone calls, and contact on social media platforms. The criminal fraudsters also use a variety of payment systems to receive that money, including person-to-person (P2P) transfer services, crypto-assets, bank-to-bank wire transfers, bank transfers through Zelle, checks, and gift cards. Each of these systems has a role to play in keeping criminals out, preventing fraud, and protecting consumers. Fraud does not succeed if the fraudster cannot contact a victim or if the fraudster cannot receive the money.

Fraud may result in unauthorized transactions or fraudulently induced transactions, each with different protections. After obtaining information through phishing schemes, fraud schemes, or data breaches, criminals may make unauthorized transactions for which consumers generally have protection (though, in some cases, imperfect protection, as discussed below). Checks can also be stolen and altered, another form of unauthorized transaction. Or criminals can defraud a consumer into making a fraudulently induced transaction where protection is sorely lacking.

As discussed in more detail below, payment fraud usually involves at least two institutions – the institution that holds the fraud victim's account (the consumer's institution)¹⁴ and the institution

¹⁴ Though businesses can also be the victims of fraud, this testimony will focus on consumers and consumer protection.

that receives the stolen funds and holds the account of the fraudster or money mule (the receiving institution). When seeking to prevent and remedy fraud, it is important to focus on the responsibilities of both the consumer's institution and the receiving institution as well as the payment system itself, regardless of whether the fraud is unauthorized or fraudulently induced. When consumers are protected, these institutions and systems will have incentives to use their resources and technological innovations to prevent fraud and make everyone safer.

III. Person-to-Person (P2P) Payment Fraud.

A. The prevalence of P2P use and the incidence of fraud on these platforms.

Person-to-person (P2P) payment apps have become increasingly popular among consumers. According to the Atlanta Federal Reserve, as of 2023, almost three-quarters of U.S. consumers used payment accounts such as PayPal, Venmo, Zelle, and Cash App in 2023.¹⁵ In addition to P2P payment services, consumers are also increasingly adopting other forms of technology to make payments.¹⁶ P2P payment systems, if properly designed, can provide broad benefits to consumers. But those benefits will only be realized if the systems are safe to use.

According to the FTC, "payment app or service" is the second largest category of payment method specified by fraud victims in terms of number of reports (after credit cards) for all of 2024, and the largest category of payment method specified by fraud victims in terms of number of reports for the first two quarters of 2025.¹⁷ The Consumer Financial Protection Bureau (CFPB) has also seen high growth in complaints about fraud in P2P apps and digital wallets.¹⁸

As consumer, small business, civil rights, community, and legal service groups described at greater length in comments submitted to the Federal Reserve Board (FRB) and the CFPB, the existing P2P payment systems of large technology companies and financial institutions simply are not safe for consumers to use.¹⁹ The news media has reported many of the fraudulent

¹⁵ Federal Reserve Bank of Atlanta, *2023 Survey and Diary of Consumer Payment Choice: Summary Results*, (June 2024), available at https://www.atlantafed.org/-/media/documents/banking/consumer-payments/survey-diary-consumer-payment-choice/2023/sdpc_2023_report.pdf.

See Federal Trade Commission, *New FTC Data Show Consumers Reported Losing Nearly \$8.8 Billion to Scams in 2022*, (Press Release) (February 23, 2023), available at <https://www.ftc.gov/news-events/news/press-releases/2023/02/new-ftc-data-show-consumers-reported-losing-nearly-88-billion-scams-2022>.

¹⁶ Chen, Jane, Deepa Mahajan, Marie-Claude Nadeau, and Roshan Varadarajan, "Consumer Digital Payments: Already Mainstream, Increasingly Embedded, Still Evolving," Digital Payments Consumer Survey, (October 20, 2023), available at <https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/consumer-digital-payments-already-mainstream-increasingly-embedded-still-evolving>.

¹⁷ FTC fraud reports by payment method, available at <https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods>. The FTC can identify the payment method that the criminal used in only a small fraction of fraud reports, and fraud is underreported in general, so the FTC's numbers vastly understate the amount of fraud facilitated by Payment app or service.

¹⁸ U.S. PIRG Educ. Fund, *Virtual Wallets, Real Complaints*, at 2, (June 2021), available at https://uspig.org/sites/uspig/files/reports/VirtualWallets/Virtualwallets_USP_V3.pdf.

¹⁹ See Comments of 65 Consumer, Civil Rights, Faith, Legal Services and Community Groups to CFPB on Big Tech Payment Platforms at 4-5, Docket No. CFPB-2021-0017, (December 21, 2021), available at <https://bit.ly/CFPB-BTPS-comment> ("CFPB Big Tech Payment Platform Comments"); Comments of 43 consumer, small business, civil rights, community and legal service groups to Federal Reserve Board Re: Collection of Checks and Other Items by

schemes enabled by the P2P systems.²⁰ Generally, these scams and theft would not have been possible without the payment apps.

P2P fraud has a particularly harsh impact on low-income families and communities of color. These communities, already struggling and often pushed out of the traditional banking system, can least afford to lose money to scams and errors. Because many people of color and immigrant communities are also unbanked or underbanked,²¹ they are the target audience for use of many of the P2P apps. For example, a September 2022 Pew Research Center survey shows that 59% of Cash App users are Black and 37% are Hispanic.²²

Yet Cash App has also been subject to reports of widespread fraud,²³ failing to protect the very vulnerable populations it targets. As a result, 48 state regulators obtained a consent order against Block, the operator of Cash App. The CSBS order required Block to pay \$80 million and “undertake corrective action for violations of the Bank Secrecy Act (BSA) and anti-money laundering (AML) laws that safeguard the financial system from illicit use.”²⁴ Similarly, the CFPB ordered Block to pay \$175 million and to fix its failures after finding that Block failed to take timely, appropriate, and effective measures to prevent, detect, limit, and address fraud on the Cash App platform.²⁵

Zelle is another popular P2P payment service, but users transfer funds between bank accounts directly.²⁶ As more and more consumers have used Zelle, the service also has become popular among criminals.²⁷ As a result of the many complaints relating to payment fraud on Zelle, the

Federal Reserve Banks and Funds Transfers Through Fedwire, Docket No. R-1750; RIN 7100-AG16, (September 9, 2021), available at <https://bit.ly/FedNowCoalitionComments> (FedNow Comments).

²⁰ Morales, Mark, “Venmo and other payment app theft is ‘skyrocketing,’ Manhattan DA warns,” CNN, (January 23, 2024), available at https://www.cnn.com/2024/01/23/business/venmo-payment-app-theft?cid=ios_app; Johnson, Tia, “Kansas City woman warns others after losing nearly \$2,000 in rental home scam,” Fox4, (May 3, 2021), available at <https://fox4kc.com/news/kansas-city-woman-warns-others-after-losing-nearly-2000-in-rental-home-scam/>; Cioppa, Jordan, “James Island woman says rental scam cost her \$2,600,” WCBF News2, (January 10, 2023), available at <https://www.counton2.com/news/james-island-woman-says-rental-scam-cost-her-2600/>.

²¹ 11.3 percent of Black and 9.3 percent of Latino households are unbanked compared to only 2.1% of white households. See FDIC, *2021 FDIC National Survey of Unbanked and Underbanked Households*, at 2, available at <https://www.fdic.gov/analysis/household-survey/2021report.pdf> (last updated July 24, 2023).

²² Anderson, Monica, “Payment apps like Venmo and Cash App bring convenience – and security concerns – to some users,” Pew Research Center, (September 8, 2022), available at <https://www.pewresearch.org/short-reads/2022/09/08/payment-apps-like-venmo-and-cash-app-bring-convenience-and-security-concerns-to-some-users/>.

²³ Hindenburg Research, “Block: How Inflated User Metrics and ‘Frictionless’ Fraud Facilitation Enabled Insiders To Cash Out Over \$1 Billion,” (March 23, 2023), available at <https://hindenburesearch.com/block/>. (“Former employees estimated that 40%-75% of accounts they reviewed were fake, involved in fraud, or were additional accounts tied to a single individual”).

²⁴ CSBS, “State Regulators Issue \$80 Million Penalty to Block, Inc., Cash App for BSA/AML violations,” (Press Release) (January 15, 2025), available at <https://www.csbs.org/newsroom/state-regulators-issue-80-million-penalty-block-inc-cash-app-bsaaml-violations>.

²⁵ *In re. Block, Inc.*, CFPB No. 2025-CFPB-0001, (January 16, 2025) (consent order), available at https://files.consumerfinance.gov/f/documents/cfpb_block-inc-consent-order_2025-01.pdf.

²⁶ The FTC designates Zelle transfers as part of the “bank transfer or payment” category, which also includes bank-to-bank wire transfers. See Section V.A of this testimony for FTC statistics on “bank transfer or payment,” also available at

<https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods>.

²⁷ Cowley, Stacy and Nguyen, Lananh, “Senators question Zelle over how it is responding to reports of rising

CFPB filed suit against Early Warning Systems (EWS) (the operator of Zelle), Bank of America, JPMorgan Chase, and Wells Fargo, alleging violations of the EFTA and violations of the Consumer Financial Protection Act. The CFPB alleged these players knowingly rushed the launch of Zelle “without implementing effective consumer safeguards.”²⁸

However, with the change in Administration and the change of leadership at the Agency, the CFPB dismissed the suit. In the wake of the dismissal, the New York Attorney General filed suit against EWS on August 13, 2025.²⁹ The NY AG seeks restitution for New Yorkers who were harmed by Zelle, which “failed for years to set up anti-fraud features, allowing criminal fraudsters to steal more than \$1 billion from users between 2017-2023.”³⁰

B. How technology perpetuates P2P fraud and theft.

Fraudsters have extraordinary creativity; they are constantly developing creative ways to steal people’s money by setting up increasingly sophisticated schemes to obtain access to accounts or to fraudulently induce consumers into payment transactions.³¹ The Federal Communication Commission’s (FCC) website includes a Scam Glossary detailing dozens of different ways individuals and small businesses have lost money to these schemes,³² and the FCC specifically identified P2P apps as a primary means for executing scams and fraud.³³ Clearly, the warnings provided by the payment apps themselves to beware of scams and fraud are not adequate to protect consumers from the losses.

Additionally, with imposter scams topping the FTC’s category of fraud type for the last five years,³⁴ the use of deep fakes generated by artificial intelligence (AI) to perpetuate payment

fraud,” New York Times, (April 26, 2022), available at <https://www.nytimes.com/2022/04/26/business/zelle-fraud.html>; Pradelli, Chad, “‘I still don’t know how they got access’: Woman loses thousands after thief targets her Zelle app,” ABC Action News, WMPVI-TV Philadelphia, PA (June 2, 2023), available at <https://6abc.com/zelle-peer-to-peer-payment-apps-theft-auto-payments/13335405/>; See CBS This Morning, “Complaints against mobile payment apps like Zelle, Venmo surge 300% as consumers fall victim to more money scams,” CBS News, (June 23, 2021), available at <https://www.cbsnews.com/news/venmo-payal-zelle-cashapp-scams-mobile-payment-apps/>.

²⁸ CFPB, “CFPB Sues JPMorgan Chase, Bank of America, and Wells Fargo for Allowing Fraud to Fester on Zelle,” (Press Release) (December 20, 2024), available at <https://www.consumerfinance.gov/about-us/newsroom/cfpb-sues-jpmorgan-chase-bank-of-america-and-wells-fargo-for-allowing-fraud-to-fester-on-zelle/>.

²⁹ *People of the State of New York v. Early Warning Services*, (Supreme Court of the State of New York, County of New York), complaint available at <https://ag.ny.gov/sites/default/files/court-filings/people-of-the-state-of-new-york-v-early-warning-services-llc-complaint-2025.pdf>.

³⁰ New York State Attorney General, *Attorney General James Sues Company Behind Zelle for Enabling Widespread Fraud*, (Press Release) (August 13, 2025), available at <https://ag.ny.gov/press-release/2025/attorney-general-james-sues-company-behind-zelle-enabling-widespread-fraud>.

³¹ See NCLC, EPIC report *Scam Robocalls: Telecom Providers Profit*, at 6-10, (June 2022), available at <https://www.nclc.org/wp-content/uploads/2023/02/Robocall-Rpt-23.pdf> for examples of the types of scams utilized by robocalls and scam texts; see also Testimony of Margot Saunders, NCLC “Protecting Americans from Robocalls,” Hearing Before the U.S. Senate Committee on Commerce, Science & Transportation, (October 24, 2023), available at <https://www.nclc.org/wp-content/uploads/2023/10/Testimony-of-NCLC-on-Robocalls-2023.pdf>.

³² Federal Communications Commission, Scam Glossary, available at <https://www.fcc.gov/scam-glossary>.

³³ Federal Communications Commission, “As More Consumers Adopt Payment Apps, Scammers Follow,” (updated February 25, 2021), available at <https://www.fcc.gov/more-consumers-adopt-payment-apps-scammers-follow>.

³⁴ Federal Trade Commission Fraud Reports by Report Type, Top Reports, available at <https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudLosses>.

fraud is disconcerting.³⁵ NCLC joined numerous nationwide and state advocacy organizations in sending a letter to the FTC and the CFPB on the threat of AI-generated deep fakes used for financial fraud.³⁶

C. Current ambiguity in the law leaves consumers insufficiently protected from P2P fraud.

The Electronic Fund Transfer Act (EFTA) and its implementing Regulation E protect consumers when problems with electronic funds transfers, such as P2P transactions, occur. The law provides consumers with remedies for P2P fraud when it is unauthorized, such as when a criminal defrauds a person into turning over account credentials and then the criminal commits an unauthorized transfer. The definition of “unauthorized transfer” under Regulation E is a transfer from a consumer’s account “initiated by a person *other than the consumer* without actual authority to initiate the transfer and from which the consumer receives no benefit.”³⁷

However, the response to consumer complaints about unauthorized payments by some of the largest players in the P2P market is inconsistent at best and possibly non-compliant.³⁸ It is unfortunately too common for financial institutions to fail to comply with the unauthorized use protections of the EFTA and deny reimbursement on improper grounds.³⁹

The response to P2P payment fraud becomes even more problematic when it involves claims of

³⁵ See FBI, Public Service Announcement Alert Number: I-120324-PSA “*Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud*,” (December 3, 2024), available at <https://www.ic3.gov/PSA/2024/PSA241203>; U.S. Department of Homeland Security, *Increasing Threat from Deepfake Identities*, (2021), available at https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf. See also van der Linde, Ileana, *AI scams, deep fakes, impersonations ... oh my!* JPMorgan Wealth Management, (July 10, 2025), available at <https://www.jpmorgan.com/insights/fraud/fraud-protection/ai-scams-deep-fakes-impersonations-oh-my>; Schwartz, Christopher and Wright, Matthew, “*Voice Deepfakes Are Calling. Here's How to Avoid Them*,” Gizmodo, (March 24, 2023), available at <https://gizmodo.com/ai-deepfake-voice-how-to-avoid-spam-phone-calls-1850245346>; ³⁶ NCLC et al., *Letter to CFPB and FTC on Threat of AI-Generated Deep Fakes Used for Financial Fraud*, (September 13, 2023), available at <https://www.nclc.org/wp-content/uploads/2023/10/Deepfake-based-financial-fraud-letter-to-CFPB-and-FTC.pdf>.

³⁷ 12 C.F.R. § 1005.2(m) (emphasis added).

³⁸ Brown, Sherrod, Elizabeth Warren, and Jake Reed, “*Brown, Reed, Warren Urge Venmo, Cash App to Reimburse Victims of Fraud and Scams* | United States Committee on Banking, Housing, and Urban Affairs,” (December 14, 2023), available at <https://www.banking.senate.gov/newsroom/majority/brown-reed-warren-urge-venmo-cash-app-to-reimburse-victims-of-fraud-and-scams>. See also Hindenburg Research Report, “*Block: How Inflated User Metrics and ‘Frictionless’ Fraud Facilitation Enabled Insiders to Cash Out Over \$1 Billion*,” (March 23, 2023), available at <https://hindenburgresearch.com/block/>.

³⁹ See, e.g., CFPB, Supervisory Highlights at 17, (Summer 2022) (“Examiners continued to find issues with financial institutions failing to follow Regulation E error resolution procedures.... A financial institution cannot require a consumer to file a police or other documentation as a condition of initiating or completing an error investigation.”); CFPB, Supervisory Highlights at 15, (Summer 2021), available at www.consumerfinance.gov (stating that “Supervision continues to find violations of EFTA and Regulation E that it previously discussed in the Fall 2014, Summer 2017, and Summer 2020 editions of Supervisory Highlights, respectively,” (Listing several violations)); Sonbuchner, Scott, Examiner, Fed. Reserve Bank of Minneapolis, *Consumer Compliance Outlook, Error Resolution and Liability Limitations Under Regulations E and Z; Regulatory Requirements, Common Violations, and Sound Practices*, (2d issue 2021), available at www.consumercomplianceoutlook.org.

fraudulently induced payments. P2P apps disclaim responsibility to protect consumers from fraudulently induced transactions, even though those payments go to accounts held at the same P2P app. Similarly, most banks will deny a claim of error for a fraudulently induced transaction, though Zelle has begun reimbursing consumers for some fraudulently induced transactions resulting from certain types of imposter scams.⁴⁰

The definition of “unauthorized transfer” under Regulation E as described above contemplates a transaction that was not initiated by the consumer. If the consumer initiated the transfer, even if the consumer was defrauded into initiating the payment, financial institutions are likely to dispute their liability and may even refuse to help.

Nevertheless, some fraudulently induced transactions may fall under Regulation E’s separate error protections, such as the protection against incorrect transactions – i.e., a payment that went to an imposter – or the right to obtain information.⁴¹ The CFPB also has authority to define additional categories of error.⁴²

The disparity of treatment between unauthorized and fraudulently induced payments under Regulation E is made clear in the following two scenarios:

- *Scenario A: Laurie receives a call from a person claiming to be with the IRS. The caller threatens to arrest her if she does not make a payment. Laurie gives the caller her bank account number and routing number, and the caller uses that information to initiate a preauthorized ACH debit against her account.*
- *Scenario B: Laurie receives a call from a person claiming to be with the IRS. The caller threatens to arrest her if she does not make a payment. Laurie takes out her smartphone and sends a P2P payment to the number or email given by the caller.*

Though there is very little difference in these two scenarios, Regulation E protects Laurie in Scenario A where she can contest the debit as unauthorized. In Scenario B, financial institutions will take the position that Laurie is unprotected because she initiated the payment. The difference between how the payment was initiated in Scenario A and B does not make a scammer any more entitled to the money or make the scammer’s bank any less responsible for banking a scammer.

D. Responsibility of receiving institutions.

As discussed earlier, payments often involve two institutions: the one that sent the payment (the consumer’s institution in the P2P context) and the one that received it. While the EFTA governs only the responsibilities of the consumer’s institution, other laws and network rules give the receiving institution obligations to prevent fraud.

Scenario A described above is unlikely to occur because scammers like the fake IRS caller would be deterred from using the ACH system. The ACH system vets and monitors who is

⁴⁰ Campisi, Natalie, “Scammed Out Of Money On Zelle? You Might Be Able To Get It Back,” *Forbes*, (November 13, 2023), available at <https://www.forbes.com/advisor/money-transfer/zelle-users-refunded-after-scams/>.

⁴¹ 15 U.S.C. § 1693f(f)(2), (6); 12 C.F.R. § 1005.11(a)(1)(ii), (vii).

⁴² 15 U.S.C. § 1693f(f)(7).

allowed to initiate ACH payments, and the liability of a bank that initiates and receives fraudulent debit payments under both Regulation E and NACHA rules leads to stronger controls that are more likely to keep the scammer from having an account or having access to the ACH system.

But with the growth of payment apps, online bank account opening, and identity theft, it is easier for scammers to obtain accounts – potentially using stolen or synthetic identities – that they can then use to receive payments (directly or through money mules). Yet at present, the payment service or bank receiving the fraudulent payment on behalf of the scammer has no direct liability for enabling the scammer to receive the payment. As a result, that institution has less incentive to prevent the scammer from obtaining an account, put a hold on access to suspicious payments, or shut down the account quickly.

If consumers had more remedies against fraudulently induced transactions, payment network rules could pass liability in whole or in part back to the institution that holds the fraudster or money mule account, which would help to correct these incentives. This is what the United Kingdom has done, as discussed below.

Consumer complaints of P2P fraud will continue to escalate because the current systems impose insufficient responsibility on system operators and financial institutions to protect consumers against fraudulent schemes. Given what we know about how fraudsters target opportunities with the least resistance, it stands to reason that fraudulently induced payment fraud will continue to plague P2P systems if payment systems and financial institutions are allowed to operate under the assumption that they are not liable.

E. Problems with P2P apps when consumers make mistakes.

Beyond fraudulently induced payments and unauthorized payments, P2P payment apps and financial institutions typically refuse to help consumers who accidentally send money to the wrong person or the wrong account – mistakes that are easy to make in payment services designed for convenience and speed over safety. For example, consumers can send money through P2P systems using nothing more than a cell phone number to identify the recipient.

Here are other examples:

- An employee of NCLC unexpectedly saw \$1,000 arrive in his bank account through Zelle. A few minutes later, he received a frantic phone call from a man telling him that he had put in the wrong cell phone number and asking for the money back. The NCLC employee wanted to return the money but asked his bank for assurances that it was not a scam. The man also called his bank. Both banks (each large top-10 institutions) refused to help correct the error. After weeks of getting nowhere, the NCLC employee returned the funds on faith.
- Arthur Walzer of New York City tried to send his granddaughter \$100 through Venmo as a birthday present, but instead sent it to a woman with the same first and last name. When he discovered the error, he told his bank to refuse payment of the \$100, and in response

Venmo froze his account and demanded that he pay them. Venmo eventually refunded him, but only after a journalist contacted the company on his behalf. It was the first time he had ever used Venmo – he set up an account specifically to give his granddaughter the gift.⁴³

Regulation E imposes the duty to investigate and resolve “errors,” which includes “an incorrect electronic fund transfer to or from the consumer’s account.”⁴⁴ Nothing in the EFTA excludes consumer errors, and Regulation E should be interpreted to cover them. When a payment is sent to the wrong person or in the wrong amount, the person receiving the payment is not more entitled to the payment because the error was caused by the sender. But today, most consumers are out of luck in this situation unless their bank decides to help and the receiving bank or payee is cooperative.

F. Potential remedies to address P2P payment fraud.

1. Update the Electronic Funds Transfer Act.

The EFTA was enacted 43 years ago and as described above does not directly address many of the most important issues in the current consumer payment ecosystem. The statute was initially adopted at a time when consumers were conducting business with their own financial institutions and were using payment systems that did not lead to the same types of problems that plague today’s P2P systems.

We support legislative efforts to address the many gaps and ambiguities in the Electronic Fund Transfer Act that leave consumers unprotected. Some of these problems could also be addressed by rulemaking or guidance from the CFPB, though Congressional action would be faster and less subject to challenge.

The problem of fraudulently induced electronic transfers in P2P payments could be addressed by amending the EFTA to protect consumers from liability when they are defrauded into initiating a transfer and allow the consumer’s financial institution, after crediting the consumer for a fraudulent transfer, to be reimbursed by the financial institution that allowed the scammer to receive the fraudulent payment.

Problems when consumers make mistakes could also be addressed by clarifying that the EFTA’s error resolution procedures apply when the consumer makes a mistake, such as in amount or recipient.

2. Consider the United Kingdom as an example.

The United Kingdom (UK) was early to launch real time payments, and fraudulently induced payment fraud (what the UK calls authorized push payment or APP fraud) immediately

⁴³ See Elliott, Christopher, “A Venmo user sent \$100 to the wrong person. Then the payment service froze his account,” Seattle Times, (November. 2, 2020), available at <https://www.seattletimes.com/life/travel/a-venmo-user-sent-100-to-the-wrong-person-then-the-payment-service-froze-his-account-travel-troubleshooter/>.

⁴⁴ 15 U.S.C. § 1683f(f)(2); 12 C.F.R. § 1005.11(a)(1)(ii).

followed. The UK has been formally considering how to tackle the problem of P2P fraud since 2016, when the consumers association “Which?” submitted a “super-complaint”⁴⁵ to the United Kingdom’s Payments Systems Regulator (PSR).⁴⁶ The complaint identified the problem of APP fraud, which happens when scammers deceive consumers or individuals at a business to send them payment under false pretenses to an account controlled by the scammer. Which? also identified the lack of consumer protection for victims of APP fraud.

In response, a steering group was formed, comprised of regulators, consumer advocates, financial services providers and industry representatives.⁴⁷ The result was the creation of an industry code called the Contingent Reimbursement Model (CRM) Code, launched in 2019. The CRM Code required signatories to reimburse consumers who were the victims of APP fraud under certain circumstances.⁴⁸ The CRM Code was voluntary and existed to help financial institutions in the UK, “detect, prevent and respond to APP scams.”⁴⁹

The voluntary decision of the leading UK payment industry players to develop a system to reimburse fraud victims shows the consensus that protecting consumers benefits industry players and the payment systems as a whole, not merely consumers. But the uneven implementation of the system – and the growing calls to make it mandatory – also show the limits of voluntary measures.

As reported in September 2021, very few victims of APP fraud were reimbursed under the CRM Code: “banks found victims at least partly responsible in 77% of cases assessed in the first 14 months following the introduction of a Contingent Reimbursement Model and voluntary code.”⁵⁰ Two banks found the customer fully liable in 90% of their decisions.⁵¹

Under the CRM code, consumers who were unhappy with their bank’s refusal to compensate them could appeal to the Financial Ombudsman Service, which reviewed denials of reimbursement requests for APP fraud. Data obtained by Which? found that in 73% of the complaints the ombudsman received about APP fraud from 2020-2021, the ombudsman concluded that banks were getting the decisions wrong, reversed the banks’ denials, and found in

⁴⁵ A super-complaint may be made by a designated consumer body where the body considers features of a market in the United Kingdom for payment systems that are or which may be significantly damaging to the interests of consumers. <https://www.gov.uk/government/publications/super-complainants-for-the-payment-systems-regulator>.

⁴⁶ As part of the Financial Services (Banking Reform) Act of 2013, the Payment Systems Regulator (PSR) was established to promote competition, innovation, and responsiveness of payment systems and to receive and respond to super-complaints. <https://www.gov.uk/government/publications/super-complainants-for-the-payment-systems-regulator>.

⁴⁷ Speech by the Lending Standards Board Chief Executive, Emma Lovell, “*International Perspective-Scams: Looking Forward: Priorities and opportunities*,” (March 15, 2022), available at <https://www.lendingstandardsboard.org.uk/scams-looking-forward-priorities-and-opportunities-international-perspective-speech/>.

⁴⁸ *Id.*

⁴⁹ *Id.*

⁵⁰ “Banks called to account over ‘shockingly low’ rate of reimbursements for APP fraud,” Finextra, (September 15, 2021), available at <https://www.finextra.com/newsarticle/38832/banks-called-to-account-over-shockingly-low-rate-of-reimbursements-for-app-fraud>

⁵¹ *Id.*

favor of the consumer.⁵² This level of reversals suggests that the banks' high rate of denials was inconsistent with both the letter and the spirit of the Code.⁵³

The Contingent Reimbursement Model as an industry response, though laudable and necessary, proved insufficient to address the growing number of scams and fraud. In the first half of 2021, APP fraud cases in the UK outnumbered credit card fraud for the first time.⁵⁴

Consequently, the UK Parliament's Treasury Committee recommended "mandatory refunds" to victims of APP fraud and discussion about whether to make "big technology companies liable to pay compensation when people are tricked by con-artists using their platforms."⁵⁵ As a result, the Payment Systems Regulator (PSR) undertook rulemaking, subject to a period of open comment ("consultation").

In June 2023, the PSR finalized a rule that requires mandatory reimbursement to victims of APP fraud.⁵⁶ Under the finalized rule as amended in 2024, victims are reimbursed up to a maximum of £85,000, with the victim's financial institution and the recipient's financial institution splitting the cost of reimbursement 50:50.⁵⁷

3. When liability is split between sending and receiving institutions and not pushed onto consumers, more will be done to protect consumers.

P2P apps must take more responsibility to protect consumers from the fraud committed on their platforms and from the scammers they allow to open accounts where they can receive stolen funds.⁵⁸ While consumer education is important and necessary, payment system providers' primary response to fraud and errors in P2P systems should not be to use old-fashioned disclosures and warnings to consumers to "be careful" and not to send payments to people they do not know—all while promoting their systems for broad use. Scammers prey on consumers'

⁵² Which?, "Banks wrongly denying fraud victims compensation in up to 8 in 10 cases," (November 11, 2021), available at <https://www.which.co.uk/news/2021/11/banks-wrongly-denying-fraud-victims-compensation-in-up-to-8-in-10-cases/>.

⁵³ Contingent Reimbursement Model Code for Authorised Push Payment Scams OP1 at 2, (April 20 2021), available at <https://www.lendingstandardsboard.org.uk/wp-content/uploads/2022/03/CRM-Code-LSB-April-2021.pdf>

⁵⁴ "UK Government to Legislate for Mandatory Reimbursement of App Fraud," (November 18, 2021), available at <https://www.finextra.com/newsarticle/39245/uk-government-to-legislate-for-mandatory-reimbursement-of-app-fraud>

⁵⁵ "Fraud: MPs seek overhaul to tackle financial scammers," (February 2, 2022), available at <https://www.bbc.com/news/business-60216076>.

⁵⁶ Press Release: "PSR confirms new requirements for APP fraud reimbursement," (July 6, 2023), available at <https://www.psr.org.uk/news-and-updates/latest-news/news/psr-confirms-new-requirements-for-app-fraud-reimbursement/>.

⁵⁷ To view a summary of the original rule and the feedback received during the open consultation, go to <https://www.psr.org.uk/media/iolpbw0u/ps23-3-app-fraud-reimbursement-policy-statement-final-june-2023.pdf>. See also Payment Systems Regulator, Cost benefit analysis, Faster Payments APP scams reimbursement requirement: changing the maximum level of reimbursement (Oct. 2024), available at <https://www.psr.org.uk/publications/policy-statements/ps247-faster-payments-app-scams-reimbursement-requirement-confirming-the-maximum-level-of-reimbursement/>.

⁵⁸ See Sanchez-Adams, Carla, "It is essential that we protect consumers from fraud over P2P networks," American Banker, Bank Think, (March 15, 2023), available at <https://www.americanbanker.com/opinion/it-is-essential-that-we-protect-consumers-from-fraud-over-p2p-networks>.

trust, and warnings are far less effective than sophisticated systems that payment providers can design.

The providers of P2P payment apps and payment systems as well as the financial institutions who utilize these applications make decisions about what safety features to install, when to protect consumers, and how to monitor and react to red flags of potentially fraudulent payments sent and received by their customers. Companies that are incentivized to prevent fraud and errors will use constantly improving technology and innovations to spot potential scams and errors and to aggregate reports of fraud. Because the UK's new rule will require financial institutions to compensate consumers affected by fraudulently induced transfers (APP scams), for example, nine of the UK's biggest banks have signed up to use a new AI-powered tool that helps banks more effectively spot if their customers are sending money to fraudsters.⁵⁹

Furthermore, financial institutions already have "Know Your Customer" (KYC) and account monitoring obligations under the Bank Secrecy Act (BSA) and Anti-Money Laundering (AML) laws, which should be reflected through their Customer Identification Program (CIP) and Customer Due Diligence (CDD) policies. Even P2P payment apps and fintech companies have certain obligations under the BSA. To comply with these laws, the institutions make decisions about who they allow to open an account and how to monitor and react to red flags of potentially fraudulent payments sent and received by their customers. When they fail in those responsibilities and allow a customer to use an account to receive stolen funds, it is appropriate for that institution to bear the costs if the funds cannot be recouped.

The responsibility of the payment service is even greater in "closed-loop" systems like Cash App, PayPal and Venmo, where one company has access to the accounts of both the consumer sending payment and the criminal fraudster receiving the payment. The P2P company benefits from having the business of both accounts and holds these funds until the consumer or the criminal fraudster chooses to move the funds. As a result, the P2P company has greater visibility into both ends of the transaction and a greater ability to assess whether the transaction is fraudulent. The company also controls the criminal fraudster's or money mule's account and can choose to freeze or hold funds while investigating a claim of fraud. The P2P company can ensure that the money stays within its system, and then reimburse the consumer who has been defrauded.

If fraud and error rates are low in the aggregate, the system can bear those costs and spread them. If rates are high, then the systems clearly have fundamental problems that must be addressed. But even a single instance of fraud or mistake can be devastating to a consumer. The equities strongly favor protecting consumers with the same type of strong protection they have in the credit card market.

⁵⁹ Solon, Olivia "Nine British Banks Sign Up to New AI Tool for Tackling Scams," Bloomberg (Jul. 25, 2023) available at <https://www.bloomberg.com/news/articles/2023-07-05/mastercard-s-ai-tool-helps-nine-british-banks-tackle-scams>.

4. Address the lack of oversight for certain parties involved in the payments market.

Newer fintech companies, including technology providers and payment apps, do not receive the same type of supervision as other financial institutions in the United States. Greater supervision of these companies would allow the supervising agency to ensure P2P companies comply with their Bank Secrecy Act obligations, are not enabling fraud, and respond appropriately to EFTA disputes by consumers, before widespread harm occurs. Greater supervision is important because compliance with basic EFTA obligations has been problematic even in supervised financial institutions, as noted above.

The CFPB had finalized a rule that would have enabled it to supervise large market participants who provide general-use digital consumer payment applications,⁶⁰ which NCLC vigorously supported.⁶¹ However, the final rule was overturned in May 2025 by a Congressional Review Act resolution.⁶² The CFPB has also all but ceased to function and has been actively dropping enforcement cases, halting supervision, and shedding responsibility over nonbanks. While state regulators have a role to play in supervising P2P companies, state regulators cannot ensure that consumers are safe in every state, have limited resources, do not have expertise in the EFTA and other federal laws, and do not have supervisory authority over national banks.

With the passage of the GENIUS Act, the Office of the Comptroller of the Currency (OCC) may have some oversight of these P2P companies in some circumstances. For example, PayPal, which operates as a P2P payment app, has also issued its own stablecoin, PayPal USD. It may very well apply for a license to be a federal qualified payment stablecoin issuer subject to supervision by the OCC. However, it is not clear if that supervision will extend to activities involving fiat payments or other types of crypto-assets, and the OCC is not focused on enforcing consumer protection laws.

IV. Fraud through Crypto-Assets.

A. Crypto-assets are a common payment method for criminal fraudsters.

According to the FTC, “cryptocurrency” is the second largest category of payment method reported by fraud victims in terms of number of dollars lost (after bank transfer or payment) for all of 2024 and the first two quarters of 2025.⁶³ Sometimes these two types of transactions are linked— for example, a fraud victim sends money to a criminal fraudster or the fraudster hacks into the victim’s account and sends the money via bank-to-bank wire transfer to an account on a

⁶⁰ The CFPB issued a final rule on November 21, 2024. It was published in the Federal Register on December 10, 2024 and the effective date was January 9, 2025. See 89 FR 99582 (December 10, 2024).

⁶¹ NCLC et al., *Comments to the CFPB’s Proposed Rule Defining Larger Participants of a Market for General-Use Digital Consumer Payment Applications*, (January 8, 2024), available at <https://www.nclc.org/wp-content/uploads/2024/01/240108-CFPB-Payments-App-Comment-Final.pdf>.

⁶² S.J. Res. 28, signed by President Trump (P.L. 119-11).

⁶³ FTC fraud reports by payment method, available at <https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods>. The FTC can identify the payment method that the criminal used in only a small fraction of fraud reports, and fraud is underreported in general, so the FTC’s numbers vastly understate the amount of fraud facilitated by crypto-assets.

crypto exchange like Coinbase. NCLC has heard of various consumers being harmed by unauthorized wire transfers to crypto accounts due to account takeovers.

Another type of fraud involving crypto-assets involves cryptocurrency kiosks, also known as “crypto ATMs,” “BTMs,” or “virtual currency kiosks”. These can be found in supermarkets, convenience stores, gas stations, bars, and restaurants, and look like bank ATMs. The crypto ATMs allow people to conduct cryptocurrency transactions, such as sending money to digital wallets, but are increasingly used as a way for criminal fraudsters to receive funds from fraud victims. A criminal will instruct their victim to withdraw cash from their own bank and deposit it into a crypto kiosk to buy a crypto-asset (virtual currency) as part of a tech support, extortion, or government impersonator scam. The crypto-asset is then sent to the scammer’s digital wallet, where it can be difficult for the stolen funds to be recovered.

The FBI reported that it received more than 10,956 complaints reporting the use of crypto ATMs kiosks in 2024, with reported victim losses of approximately \$246.7 million, a 99% increase in the number of complaints and a 31% increase in reported victim losses from 2023.⁶⁴ Amy Nofziger, director of fraud victim support at the AARP Fraud Watch Network, said “the number of victim reports involving crypto kiosks that come through AARP’s fraud helpline is ‘just overwhelming.’”⁶⁵ Nofziger also related a story about a 76-year-old fraud victim who lost her entire savings to a crypto ATM.⁶⁶

B. Crypto companies must be subject to the same BSA requirements as banks.

I will not address the safety and soundness issues posed when banks engage with the crypto industry or questions about whether particular crypto firms should or should not be allowed bank accounts. However, as Congress considers legislation to regulate the market for crypto-assets, it is essential that crypto companies and platforms be required to conduct full BSA compliance. Crypto-assets are one of the top vectors for fraud and other illegal activity, and the growth of the crypto industry will only result in more fraud if strict controls are not built in.

⁶⁴ FBI, IC3, “Internet Crime Report 2024” (“2024 IC3 Report”) at 36, available at https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

⁶⁵ Paulin, Emily, and Snow, Molly, “Scammers Are Using Crypto ATMs to Steal Millions. AARP Is Fighting Back,” AARP (Published June 10, 2024, Updated June 10, 2025), available at <https://www.aarp.org/advocacy/states-crack-down-crypto-atm-2024/>.

⁶⁶ *Id.* “Attempting to access her recently deceased husband’s Apple account, the widow mistakenly contacted an Apple customer service impersonator who convinced her that her identity had been stolen. The impersonator told her to withdraw her savings and deposit the cash into a crypto kiosk for protection. The woman withdrew \$30,000, put it into the machine and hasn’t had access to the money since.”

Enforcement of BSA requirements is essential to prevent crypto-assets from being used to perpetrate criminal activity. Both federal⁶⁷ and state regulators⁶⁸ have appropriately brought enforcement actions against crypto players that had lax programs to conduct due diligence on their customers, monitor transactions, and report suspicious activities.

Vigilant BSA oversight of accounts involving crypto-assets is also important as crypto-assets make their way into the U.S. banking and payments system. Several large, well-capitalized crypto firms have made it clear that their business model is focused on making crypto and blockchain-based ledgers a mainstream payment method for American consumers. For example, at least one major payment provider has created a stablecoin expressly intended to facilitate consumers' purchase of household goods and services,⁶⁹ while another crypto "native" firm has created a platform where retail merchants are provided crypto wallets that can receive direct crypto payments from customers, without the need to convert crypto assets into fiat currency to settle the transaction.⁷⁰ Reports claim that the platform processes payments for thousands of merchants, for "on-chain" payments worth billions of dollars.⁷¹ BSA/AML compliance is essential to ensure that "purchases" using crypto-assets are not used to enable criminals to receive stolen funds or conduct criminal activity.

Although the GENIUS Act did provide that permitted payment stablecoin issuers will be treated as financial institutions under the Bank Secrecy Act,⁷² not all crypto-assets and crypto companies are covered by the GENIUS Act. Consumers also need protection when crypto-assets are used for payments,⁷³ as discussed below.

⁶⁷ See, e.g., U.S. Dep't of Treasury, Press Release, "U.S. Treasury Announces Largest Settlements in History with World's Largest Virtual Currency Exchange Binance for Violations of U.S. Anti-Money Laundering and Sanctions Laws," (November 21, 2023), available at <https://home.treasury.gov/news/press-releases/jy1925>; FinCEN, *FinCEN Announces \$29 Million Enforcement Action Against Virtual Asset Service Provider Bittrex for Willful Violations of the Bank Secrecy Act*, (Press Release) (October 11, 2022), available at <https://www.fincen.gov/news/news-releases/fincen-announces-29-million-enforcement-action-against-virtual-asset-service>.

⁶⁸ See "Stablecoin Issuer Paxos to Pay Fine to New York for Binance Gaps," Bloomberg Law, (August 7, 2025), available at <https://news.bloomberglaw.com/crypto/stablecoin-issuer-paxos-to-pay-fine-to-new-york-for-binance-gaps> (\$48.5 million settlement for lapses in anti-money laundering adherence and other diligence failures in its partnership with Binance); N.Y. Department of Financial Services, "Superintendent Adrienne A. Harris Announces \$100 Million Settlement with Coinbase, Inc. after DFS Investigation Finds Significant Failings in the Company's Compliance Program," (Pres Release) (January 4, 2023), available at https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202301041.

⁶⁹ PayPal, "Built for stable payments. 1 USD: 1 PYUSD on PayPal," (accessed September 11, 2025), available at <https://www.paypal.com/us/webapps/mpp/digital-wallet/manage-money/crypto/pyusd>.

⁷⁰ Coinbase, "A new standard for onchain payments," (accessed September 11, 2025), available at <https://www.coinbase.com/commerce>.

⁷¹ Akolkar, Bhushan, "New Payments Protocol for Coinbase Commerce to Facilitate Instant Crypto Settlements," CoinGape (blog), (November 17, 2023), available at <https://coingape.com/new-payments-protocol-for-coinbasecommerce-to-facilitate-instant-crypto-settlements/>.

⁷² 12 USC § 5903(a)(5)(A).

⁷³ Any consumer payments made using crypto-assets should come with the full protections given to accounts under the Electronic Fund Transfer Act.

C. Stablecoins and crypto-assets must be subject to consumer protection statutes such as the EFTA when used for consumer payments.

When stablecoins or other forms of crypto-assets are used for consumer payments, they should be subject to consumer protection laws like the EFTA. In fact, some courts have found that crypto-assets are “funds” within the meaning of the EFTA. The GENIUS Act does not say otherwise, and thus does not preempt the EFTA’s protection against unauthorized transfers and errors.

Applying EFTA to the use of payment stablecoins would provide people with greater protections from payment fraud, the ability to dispute or reverse fake or erroneous transactions, and other safeguards that they have when using conventional payment instruments, such as credit cards. The CFPB should also play a role in preventing and remedying fraud that involves stablecoins and other crypto-assets.

In addition to the EFTA, consumers would also benefit from state and federal legislation aimed at addressing the harms caused to consumers from fraud schemes associated with payment by crypto ATMs, including S.710, the Crypto ATM Fraud Prevention Act of 2025. Over 20 states have already passed legislation or regulations to improve consumer protections for crypto ATMs with varying degrees of effectiveness.⁷⁴

V. Bank-to-Bank Wire Transfer Fraud.

A. Consumers are devastated by bank-to-bank wire transfer fraud.

The FTC’s latest fraud data show that “Bank Transfer or Payment” is the payment method used by criminal fraudsters to receive the largest amount of money.⁷⁵ In 2024, consumers reported losing nearly \$2.1 billion through bank transfer or payment.⁷⁶ It also seems safe to assume that the lion’s share of those losses by dollar volume are through bank-to-bank wire transfers, which can process very large transfers, rather than through Zelle, although Zelle is increasingly used for larger transfers. (The FTC’s “Wire Transfer” category includes only nonbank transfers like Western Union and MoneyGram.)

Moreover, some of the over \$1.4 billion reported lost through cryptocurrency may have started as bank-to-bank wire transfers to crypto banks or exchanges.⁷⁷ For example, Marjorie Bloom of Chevy Chase, Maryland, a 77-year-old retired civil servant, lost her life savings, \$661,000, through a bank-to-bank wire transfer into cryptocurrency.⁷⁸

⁷⁴ See AARP Comment to the Senate Banking Committee Digital Asset Market Structure Request for Information, (September 9, 2025), available at <https://www.aarp.org/content/dam/aarp/politics/advocacy/2025/09/aarp-response-to-banking-rfc.pdf>.

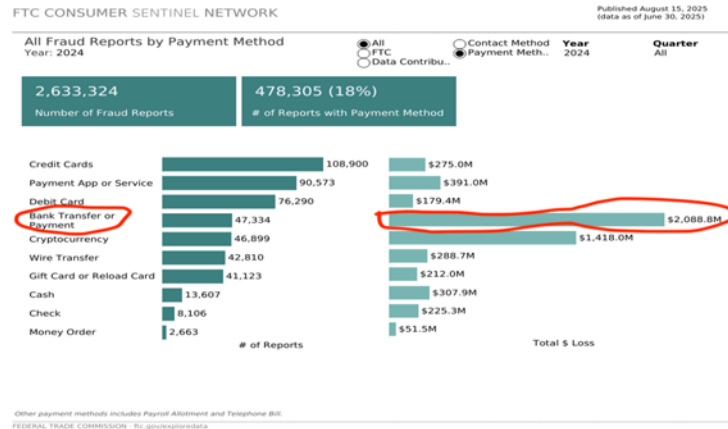
⁷⁵ FTC fraud reports by payment method available at <https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods>.

⁷⁶ *Id.*

⁷⁷ See Paluska, Michael, “Cryptocurrency scam drains retired St. Pete victim’s life savings How to spot online scams,” ABC Action News (Florida), (June 19, 2023), available at <https://www.abcactionnews.com/news/region-pinellas/cryptocurrency-scam-drains-retired-st-pete-victims-life-savings>.

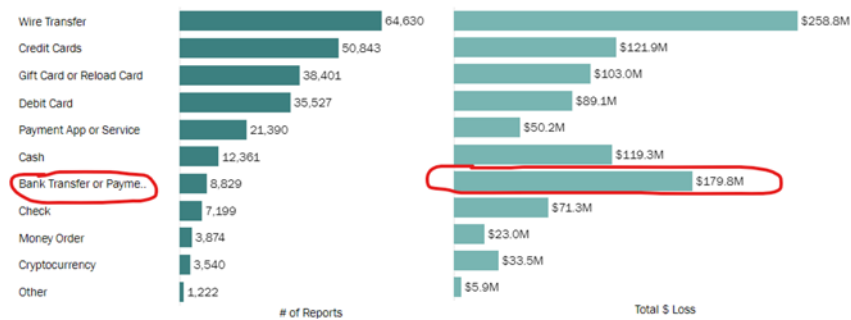
⁷⁸ Iacurci, Greg, “How this 77-year old widow lost \$661,000 in a common tech scam: ‘I realized I had been

2024 Fraud Reports to FTC Consumer Sentinel Network by Payment Method



Compared to 2019, it is especially dramatic to note how the bank transfer category has overtaken nonbank wire transfers, and how astronomically it has grown – from roughly \$180 million to almost \$2.1 billion in six years.⁷⁹

2019 Fraud Reports to FTC by Payment Method



Over the last several years, NCLC has received numerous inquiries on behalf of consumers and heard devastating reports about how criminals have used bank-to-bank wire transfers to take

defrauded of everything.” CNBC, (October 8, 2023), available at <https://www.cnbc.com/2023/10/08/how-one-retired-woman-lost-her-life-savings-in-a-common-elder-fraud-scheme.html>.

⁷⁹ The dollar losses in these two charts significantly understate actual losses, as only 12% (2019) to 18% (2024) of reports included information on payment method, and many fraud losses are not reported to the FTC.

hundreds of thousands of dollars from people. In one case, an older woman lost her home as a result. Here are other examples:

- A college student lost his entire savings account after someone with two fake identification cards went into a bank and wired \$16,500 to another individual. Busy with college, he did not notice missing money for a month and a half, but the bank refused to return the money.⁸⁰
- After a consumer was the victim of a SIM swap, a wire transfer was used to transfer \$35,000 from his bank account to an account in another state.⁸¹ He is a cancer patient and navigating the bank appeal process has been extremely stressful. These SIM swaps are increasingly common.⁸²
- A low-income consumer in New York lost over \$26,000 – all her savings, which she had carefully saved over many years – after someone transferred money from her savings account to her checking account and then made an outgoing wire transfer to another state.⁸³
- A man lost \$15,000 that was wired to another account by someone who gained access to his account. The bank spotted suspicious activity as the fraud was taking place and called the man, who alerted them to the fraud, but the bank still refused to return the money claiming that the EFTA did not apply to these fraudulent electronic transactions.
- A fraudster hacked a retiree's online banking account and made a cash advance from the retiree's credit card to his linked bank account. The fraudster then immediately wired that amount from the retiree's bank account to his own. The bank denied any relief.⁸⁴
- A small business had its online banking account hacked and its \$60,000.00 checking account balance emptied over the course of two days and six transactions. The bank denied relief because its banking agreement generally states that customers are responsible for unauthorized transactions.⁸⁵

Wire fraud has become so problematic that even large news outlets like Good Morning America have run stories about the perils and lack of protection available to impacted consumers.⁸⁶

⁸⁰ Inquiry received by KPRC (Houston NBC station) reporter Amy Davis.

⁸¹ Email from attorney on file with NCLC.

⁸² See Barr, Luke, ABC News, "'SIM swap' scams netted \$68 million in 2021: FBI" (February 15, 2022), available at <https://abcnews.go.com/Politics/sim-swap-scams-netted-68-million-2021-fbi/story?id=82900169>.

⁸³ Email from CAMBDA Legal Services to NCLC, on file with NCLC.

⁸⁴ Pending arbitration before AAA (Wells Fargo).

⁸⁵ *Lawrence and Louis Company d/b/a Hidden Oasis Salon v. Truist Bank*, No. 1:22-cv-200-RDA-JFA (E.D. Va.).

⁸⁶ ABC News, Good Morning America, "Woman sounds alarm on sophisticated wire transfer fraud," (July 21, 2023), available at <https://abcnews.go.com/GMA/Living/video/woman-sounds-alarm-sophisticated-wire-transfer-fraud-101547100>.

All the examples provided above were for unauthorized wire transfers. However, we have also heard stories where the consumer was fraudulently induced into sending a wire transfer. For example:

- Three Ohio residents were all defrauded into making a bank-to-bank wire transfer by a Chase impersonation scam.
 - Jeff Phipps from Columbus, Ohio lost \$8,500 after the fraudster, impersonating a bank employee, called and convinced the man that his account had been hacked into and he needed to provide login information to protect it. “They asked him if he had authorized a wire transfer and he replied, ‘no’. They kept him on the phone for an hour and 47 minutes. They said, ‘Well, we want to deactivate your account. Can you send us your username and your passcode?’ And he did thinking it was Chase.” The fraudster took \$8,500 with this information and Chase refused to refund the victim’s money since he had given information to the scammer, “authorizing” it.⁸⁷
 - Kelli Hinton, 7 months pregnant at the time, received a text about a fraudulent wire transfer from her account, then a follow-up call from a fraudster posing as a Chase fraud agent, spoofing Chase’s real phone number. The fraudster kept her on the line for an hour and convinced her to change her username and password, allowing him to drain \$15,000 from her account.⁸⁸
 - Just months after experiencing a near fatal collision that left him in a wheelchair, Todd Evans from West Chester Township was called by a fake Chase fraud protection agent. The fraudster told him about a fraudulent purchase from his account, which Todd confirmed was appearing on his account and which neither he nor his wife had made. The fraudster then mentioned a \$45,000 fraudulent wire transfer from the account. Todd and his wife were nervous about addressing the fraud and asked the caller to verify his identity. He asked the couple to look at the number he was calling from and verify it matched the number on their debit card. Based on this confirmation, the couple allowed the fraudster to guide them through a “wire reversal process”. Hours later they were out \$63,000.⁸⁹
- A couple in South Carolina received an email from their attorney at the time of closing their home purchase with instructions on where to send the down payment via bank-to-bank wire transfer. Their attorney had been the victim of a phishing scam, and the fraudster used a legitimate email copying an actual employee of the attorney. The couple lost \$108,000.⁹⁰

⁸⁷ Gordon, Clay, “Central Ohio man loses \$8,500 in Chase bank impersonation scam,” 10 WBNS, (March 30, 2023), available at <https://www.10tv.com/article/money/consumer/wire-fraud-scam-warning/530-7af76f5c-cc0-4dcc-98a3-5c740a9043bd>.

⁸⁸ McCormick, Erin “Gone in seconds: rising text scams are draining US bank accounts,” The Guardian, (April 22, 2023), available at <https://www.theguardian.com/money/2023/apr/22/robo-texts-scams-bank-accounts>.

⁸⁹ Johnson, Karin “West Chester couple swindled out of thousands of dollars by crooks spoofing bank’s phone number,” WLWT5 news, (November 16, 2023), available at <https://www.wlwt.com/article/west-chester-chase-bank-spoofing-phone-number/45866051>.

⁹⁰ Lee, Diane, “Upstate couple warns of wire fraud that cost them \$108,000,” CBS7 News, (May 19, 2023),

Even in instances where consumers realize they have fallen prey to a fraud scheme, banks are sometimes unwilling or unable to assist consumers or stop a wire transfer. For example, Ann Booras from San Ramon, California received a call from a fraudster impersonating a Wells Fargo employee asking if she had wired \$20,000 from her savings account. In response to the directions provided by the fake employee, Ann wired the \$20,000 sum to the “bank’s fraud department” where it would be safe. The fraudster then continued asking about other supposedly fraudulent transactions, and panicking, Ann “drove to the nearest Wells Fargo branch, with the man still on the phone, and told a teller someone was attacking her accounts. Silently, the teller warned her - the thief was actually the man on the phone. ‘I had tears running down my face, I was literally shaking because I realized I had just sent \$25,000 to who knows where.’” Ann “pleaded with bank employees to stop those wire transfers -- fast. But to her shock, no one would help.” She was told, “I’m sorry we’re all busy. We’re backed up with appointments back to back. You need to go to another branch, but we can’t help you here.”⁹¹

B. Technology enables more bank-to-bank wire transfer fraud.

As the previous stories all illustrate, fraudsters have taken advantage of the technology needed to send texts and make calls to consumers whose information has been obtained through phishing schemes or purchased from the dark web. Technology also enables fraudsters and hackers the ease to take over accounts and initiate transactions through online or mobile banking.

Previously, wire transfers had to be conducted through a cumbersome process of walking into a bank for a time-consuming, in-person transaction. In-person identification would prevent unauthorized transfers, and there were some speed bumps for fraudulently induced transactions as well—the consumer would have time to think about the situation, call a family member, and talk to the bank teller, who could potentially talk them out of it.

But increasingly, bank-to-bank wire transfers are a service offered and permitted through mobile and online banking. As a result, fraudsters have an easy method of using unauthorized or fraudulently induced transfers to steal and send large sums of money, often not possible through P2P apps that set daily transaction limits. The lack of friction that was found in in-person transactions has undoubtedly contributed to the explosion of bank-to-bank wire transfer losses.

C. Banks claim bank-to-bank wire transfers are exempt from the EFTA, leaving consumers exposed to losing thousands of dollars.

The EFTA does not directly exempt wire transfers; it exempts electronic transfers, other than ACH transfers, made “by means of a service that transfers funds held at either Federal Reserve

available at <https://www.wspa.com/news/upstate-couple-warns-of-wire-fraud-that-cost-them-108000/>.

⁹¹ Finney, Michael and Koury, Renee, “Wells Fargo bankers tell East Bay customer they’re too busy to stop wire scam,” ABC7, (June 21, 2023), available at <https://abc7news.com/bank-impostor-scam-wells-fargo-wire-transfer-fraud-scammer-pretends-to-be/13407340/#:~:text=Wells%20Fargo%20bankers%20tell%20East,busy%20to%20stop%20wire%20scam&text=The%20victim%20was%20still%20on,SAN%20RAMON%2C%20Calif>.

banks or other depository institutions and which is not designed primarily to transfer funds on behalf of a consumer.”⁹² However, Regulation E and the official interpretations of Regulation E interpret that exemption to cover wire transfers using Fedwire or through a similar wire transfer system, like SWIFT, CHIPS, and Telex, that is used primarily for transfers between financial institutions or between businesses.⁹³

Fraudulent wire transfers can cause consumers to lose their entire life’s savings. Banks claim that even if a criminal impersonates the consumer and makes a completely unauthorized wire transfer, the EFTA and Regulation E protections do not apply; instead, they assert that bank-to-bank wire transfers are covered under state law, more specifically a state’s adopted version of Uniform Commercial Code Article 4A (UCC Article 4A).

But the UCC was not designed as a consumer protection statute and was instead designed to govern commercial-to-commercial transactions. UCC Article 4A offers very weak or no protection for consumers who have suffered harm due to bank-to-bank wire transfer fraud. In essence, the consumer is deemed to have authorized a wire transfer if the bank utilized a commercially reasonable security procedure that the bank and the consumer agreed to beforehand and if the bank acted in good faith. Yet consumers have no understanding of or control over those security procedures and no choice but to click “I agree” to the fine print of an agreement. Banks also claim that their procedures are commercially reasonable even when they are inadequate.

For example, the New York Attorney General recently filed a lawsuit against Citibank alleging it failed to protect and reimburse victims of electronic fraud when it used “poor security and anti-fraud protocols” that consumers had not negotiated with Citibank.⁹⁴ According to the lawsuit, Citibank connected wire transfer services to consumers’ online and mobile banking apps in recent years—allowing direct electronic access to the wire transfer networks—but employed lax security protocols and procedures; had ineffective monitoring systems; failed to respond in real-time; and failed to properly investigate fraud claims.⁹⁵ As a result, New Yorkers lost millions of dollars in life savings, their children’s college funds, and even money needed to support their day-to-day lives.

I have also heard numerous other reports of banks failing to reimburse unauthorized wire transfers, even when the consumer did not agree to any commercially reasonable security procedure. Consumers do not have the resources to fight the bank in court or arbitration to enforce their right to a reimbursement when this occurs.

UCC Article 4A does not provide a consumer with any other remedies besides reimbursement (and possible interest) of the unauthorized wire amount, and the consumer’s attorney is not entitled to recover attorneys’ fees from the bank. As a practical matter, it means that a consumer

⁹² 15 U.S.C. §1693a(7)(B).

⁹³ Reg. E, 12 C.F.R. § 1005.3(c)(3).

⁹⁴ New York State Attorney General, “Attorney General James Sues Citibank for Failing to Protect and Reimburse Victims of Electronic Fraud,” (Press Release) (January 30, 2024), available at <https://ag.ny.gov/press-release/2024/attorney-general-james-sues-citibank-failing-protect-and-reimburse-victims>.

⁹⁵ See Complaint, *People of the State of New York v. Citibank*, No. 1:24-cv-00659 (S.D.N.Y. filed January 30, 2024), available at <https://ag.ny.gov/sites/default/files/2024-01/citi-complaint.pdf>.

would have to pay out of pocket to fight in court or in arbitration just to get their money back, while a financial institution with deep pockets can afford to fight a claim. As a result, in most cases financial institutions will reject a consumer's unauthorized wire transfer claim because the consumer cannot afford to fight the decision.

With respect to fraudulently induced wire transfers, the UCC provides no remedy.

D. Potential remedies to address bank-to-bank wire fraud.

The exemption in Regulation E should be eliminated, and until it is, it should be interpreted narrowly. When the EFTA was written in 1978, bank-to-bank wire transfers were rarely used by consumers and required an in-person visit to the bank. That has clearly changed— bank-to-bank wire transfer services are now incorporated into consumer mobile and online banking services and electronic fund transfers are generally far more common among consumers today than in 1978. For large payments, bank-to-bank wire transfers are the primary way consumers can conduct electronic transfers.

In its suit against Citibank mentioned above, the New York AG alleged that the unauthorized wire transfers that occurred by electronic requests initiated by scammers via online banking or mobile app are covered by the EFTA. The court agreed with the New York AG, holding that the wire exemption does not cover the transfer between the consumer and their bank before a service like Fedwire is used to transfer the funds.⁹⁶

As previously stated, we also support legislative efforts to address gaps in the Electronic Fund Transfer Act that leave consumers unprotected.

The EFTA can be amended to address specific problems of unauthorized consumer bank-to-bank wire transfers as well as fraudulently induced consumer bank-to-bank wire transfers by:

- Eliminating the exemption for bank wire transfers and electronic transfers authorized by telephone call, bringing those transfers within the EFTA and its protections against unauthorized transfers and errors;
- Protecting consumers from liability when they are defrauded into initiating a transfer, and
- Allowing the consumer's financial institution, after crediting the consumer for a fraudulent transfer, to be reimbursed by the financial institution that allowed the scammer to receive the fraudulent payment.

The consumer bank-to-bank wire transfer loophole and inclusion of fraudulently induced transfers could also be addressed by rulemaking or guidance from the CFPB, though Congressional action would be faster and less subject to challenge.

⁹⁶ *New York v. Citibank*, 763 F.Supp.3d 496 (S.D.N.Y. 2025).

VI. Check Fraud.

A. Check alteration fraud is on the rise.

Although checks are an old payment system, new technology is leading to a rise in fraud using checks. In particular, new technology makes it easier for criminals who steal checks to engage in “check washing” – changing the payee and payment amount on a check – and harder for banks or consumers to spot those alterations.⁹⁷ Criminals can also create fake checks from stolen account information. These altered or fabricated checks can then be deposited remotely through mobile devices, made easier through the increased ability to open fraudulent accounts into which those checks can be deposited.

Although checks are near the bottom of payment types in terms of number of fraud reports, the total dollar loss by check fraud reported to the FTC in 2024 is actually higher than for debit cards, gift cards or reload cards, and money orders. But this reported dollar loss is vastly understated,⁹⁸ one report from 2023 puts annual check fraud losses at \$815 million.⁹⁹

Also in 2023, FinCEN issued an alert about a nationwide surge in mail theft-related check fraud schemes and urged financial institutions to “be vigilant in identifying and reporting such activity.”¹⁰⁰ The report indicated that there were over 680,000 cases of possible check fraud reported to FinCEN in 2022 through the use of SARs (Suspicious Activity Reports), an increase from a little over 350,000 check fraud-related SARs sent to FinCEN in 2021, which itself was a 23% increase from 2020.¹⁰¹ The statistics for check-fraud related SARs were not specific to mail-theft related check fraud.¹⁰²

Technology also enables criminal organizations to traffic stolen checks. As a 2023 New York Times article¹⁰³ conveyed:

“The cons may start with stealing pieces of paper, but they leverage technology and social media to commit fraud on a grander scale, banking insiders and fraud experts said. In the past, criminals needed a special internet browser that would grant entry into the

⁹⁷ DePompa, Rachel, “‘Check washing’ scams still on the rise,” Fox10 News, (January 25, 2024), available at <https://www.fox10tv.com/2024/01/25/check-washing-scams-still-rise/>.

⁹⁸ Of the 2.5 million reports of fraud received by the FTC in 2022, only 17% specified the payment method for the fraud. FTC fraud reports by payment method available at <https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods>.

⁹⁹ Nadelle, David, “Check Washing Is an \$815M Per Year Scam — How It Works and Ways To Prevent It,” GoBanking Rates, (February 22, 2023), available at [https://www.nasdaq.com/articles/check-washing-is-an-\\$815m-per-year-scam-how-it-works-and-ways-to-prevent-it](https://www.nasdaq.com/articles/check-washing-is-an-$815m-per-year-scam-how-it-works-and-ways-to-prevent-it).

¹⁰⁰ FinCEN, FIN-2023-Alert003, *FinCEN Alert on Nationwide Surge in Mail Theft-Related Check Fraud Schemes Targeting the U.S. Mail*, (February 27, 2023) available at <https://www.fincen.gov/sites/default/files/shared/FinCEN%20Alert%20Mail%20Theft-Related%20Check%20Fraud%20FINAL%20508.pdf>

¹⁰¹ *Id.* citing FinCEN SAR Stats available at <https://www.fincen.gov/reports/sar-stats>

¹⁰² *Id.* See FN 10.

¹⁰³ Barnard, Tara Seigel, “We Can’t Stop Writing Paper Checks. Thieves Love That,” (December 9, 2023), available at https://www.nytimes.com/2023/12/09/business/check-fraud.html?unlocked_article_code=1.QU0.O8_m.7j3dyrD0mzvX&smid=url-share

dark web marketplace of stolen checks, maybe even someone to vouch for them. Now all they need is an account from Telegram, a messaging app.

“You can buy checks on the internet for \$45, with a perfectly good signature,” said John Ravita, director of business development at SQN Banking Systems, which provides check fraud detection software. “There is one website that offers a money-back guarantee. It’s like Nordstrom.”

NCLC spoke with Larry Smith, an attorney in Chicago, whose clients did not even have checks issued to their associated bank account, yet a fraudster somehow obtained their bank account and routing number and created fake checks.¹⁰⁴ The fraudster deposited these checks in various bank accounts from December 2021 and January 2022, stealing around \$14,000 from the consumers. Though the consumers disputed the fraudulent checks with their bank and have filed a lawsuit, their bank has not recredited their account for the stolen amount.

B. Though some protections exist for consumers harmed by check fraud, they are often left scrambling.

Checks are largely governed by state law through the Uniform Commercial Code (UCC). If a consumer timely reports the problem, the UCC protects them if their checks are altered or if a fraudulent check is presented against their account.¹⁰⁵

Yet as the previous example demonstrates, consumers are often left scrambling, waiting for their banks to recredit their account even when state law provides remedies for the consumer when a check is altered or forged. One consumer in Los Angeles was unable to get his account recredited for over two years. The consumer had written a check to the IRS and sent it by mail. The check was stolen from the mail and deposited into an account that was not the U.S. Treasury.¹⁰⁶ The consumer’s bank kept insisting it would not recredit his account until the fraudster’s bank sent them reimbursement.

While a bank’s obligation to reimburse a consumer for an altered check is not dependent on the bank’s ability to be repaid by the depository bank, the failure to timely resolve check fraud between institutions has also been the subject of complaint by community banks against their large-bank counterparts.¹⁰⁷ Consumers turn to their own bank for reimbursement when a check is altered or forged, and that bank in turn will request reimbursement from the bank into which the check was fraudulently deposited. As previously described in more detail in Section III. F. 3., the depository bank has “know-your-customer” responsibilities that are important to prevent fraud, but there is insufficient incentive to be diligent if there is no liability. As Steven Gonzalo,

¹⁰⁴ *Arroyo and Ramos v. Fifth Third Bank, N.A.*, Cause No. 2023L004163, Cook County, IL.

¹⁰⁵ See U.C.C. §§ 3-407(b), (c) cmt. 2, 4-401(d)(1) for a consumer’s rights when a check is altered; see U.C.C. §§ 4-401; 4-406(f) for a consumer’s rights when a check is forged.

¹⁰⁶ See Lazar, Kristine, “On Your Side: Check fraud is on the rise- here’s how to protect your money,” CBS News Story, KCAL News, (April 17, 2023), available at <https://www.cbsnews.com/losangeles/news/on-your-side-check-fraud-is-on-the-rise-heres-how-to-protect-your-money/>.

¹⁰⁷ Berry, Kate, “Small banks urge crackdown on big banks with lax check-fraud controls,” American Banker, (February 9, 2023), available at <https://www.americanbanker.com/news/small-banks-urge-crackdown-on-big-banks-with-lax-check-fraud-controls>

president and CEO of American Commercial Bank & Trust, stated: “From a deposit perspective, some banks do not perform the same level of due diligence because the bank assumes the risk of loss to them is zero or minimal, and fails to consider losses due to fraud incurred by the counterparty banks. And therein lies the failure.”¹⁰⁸

Furthermore, even though the UCC provides consumers up to a year to inform their bank of a fraudulent or altered check, it allows banks to shorten that notification time in the fine print of account agreements. Many bank account agreements shorten that time for notification to anywhere between 14 and 30 days.

Yet check alterations can be hard to spot. If the payee has been changed but not the amount, the consumer might have no reason to think that anything is amiss. For example, one consumer reported to NCLC that he had no idea his check had been altered until his landlord – a family friend – eventually told him months later that he had not received the rent.

Most banks no longer return physical checks to consumers and have also engaged in an aggressive push to eliminate paper statements. Bank websites and mobile apps focus on listing transactions but make it more cumbersome to review actual statements. The grainy photocopies of checks included with statements can be hard to read, consumers may not expect to have any reason to look at them, and those images are not even available to review on some mobile banking apps.

But if the consumer does not inform their bank about the check fraud before the end of the 14- to 30-day time period, they may be left with absolutely no recourse at all.

C. Potential remedies to address check fraud.

While the UCC provides remedies to consumers if a check is altered or forged check, if the drawee bank is unable to get compensation from the depository bank, the drawee bank may delay in, or sometimes even fail to comply with, their obligations under the Uniform Commercial Code (UCC) to credit the consumer’s account for a check that was not properly payable.¹⁰⁹ Thus, federal regulators should require the depository bank to swiftly compensate the drawee bank. At the same time, the federal regulators should be vigilant to ensure that drawee banks fulfill their obligations to their customers even if they have a dispute with the depository bank.

We also note that consumers need to have sufficient time to dispute a check as altered or forged. The UCC only requires that the consumer act with reasonable promptness in examining the bank statement and must promptly notify their bank¹¹⁰ no later than one year after the statement is made available.¹¹¹ But many banks shorten those timelines in the account agreement, sometimes to as short as 30 days. Yet most consumers have never heard of check washing and reasonably do not expect that they should have to examine checks for alterations or forgeries. Moreover, most banks no longer return original checks and instead make check images available, often at a

¹⁰⁸ *Id.*

¹⁰⁹ UCC § 3-407(b), (c) cmt. 2; § 4-401(d)(1); § 4-401 cmt. 1.

¹¹⁰ UCC § 4-406(c).

¹¹¹ UCC § 4-406(f).

reduced size. Those images can be extremely hard to read. That problem is compounded by the widespread elimination of paper statements, with consumers only getting an email that an online statement is available, and bank websites are generally set up to encourage viewing transactions but not statements. If the amount has not changed, the consumer may have no reason to suspect anything is wrong. Thus, we encourage federal regulators to insist that financial institutions give consumers a reasonable time to identify and report check alterations and forgeries, which may be longer than 30 days.

We also suggest that the federal Reserve Board make certain changes to Regulation CC, concerning the availability of funds from check deposits.¹¹²

In summary, to protect consumers from check fraud:

- Federal bank regulators should examine institutions to ensure that they are complying with their responsibility to reimburse consumers for altered or forged checks, and that depository banks are appropriately reimbursing drawee banks.
- Federal bank regulators should step up enforcement of BSA/AML obligations and scrutinize the institutions into which fraudulent checks are deposited.
- States should amend their UCC laws to remove the ability of banks to shorten the time period provided by the UCC to report altered or forged checks.
- Improvements in the protections for P2P payments would also give consumers more confidence in using those systems instead of checks.

We should also give consideration to moving consumer protections for checks within the EFTA, which provides a clearer framework than the UCC for consumer protection including error resolution timelines and procedures and consumer rights.

The Federal Reserve Banks should also explore collecting information on check fraud, which may help to identify institutions that need to do a better job with their BSA/AML obligations.

VII. Electronic Benefit Transfer (EBT) Card Fraud.

A. EBT card skimming and theft leave cardholders without any protections.

Supplemental Nutrition Assistance Program (SNAP) benefits are distributed and administered through the Electronic Benefit Transfer (EBT) system to eligible participants. EBT has been the sole method of SNAP issuance in all states since June of 2004,¹¹³ and some states also use EBT cards to issue Temporary Assistance for Needy Families (TANF) or other state-administered financial assistance. EBT accounts perform the same function for low-income households as do

¹¹² See NCLC, *Comments regarding the Request for Information on Potential Actions to Address Payments Fraud by the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, and Federal Deposit Insurance Corporation*, (September 15, 2025), available at https://www.nclc.org/wp-content/uploads/2025/09/2025.09.15_Comments_Fraud-RFI-on-Payments-Fraud.pdf.

¹¹³ U.S. Department of Agriculture, Food and Nutrition Service, <https://www.fns.usda.gov/snap/ebt> (last accessed September 15, 2025).

checking accounts—the accounts power daily, or near daily, transactions. People who receive these benefits typically spend down the account balance to \$0 each month.

In 2020, about 39.9 million people across the country received SNAP benefits;¹¹⁴ 38% of whom were white, 25.5% Black, and 15% Hispanic.¹¹⁵ As of 2022, nearly 2 million Americans receive Temporary Assistance for Needy Families (“TANF”) benefits to support their families.¹¹⁶ In FY 2021, 35% of TANF recipients were Hispanic, 29% were Black, and 27% were white.¹¹⁷ These public benefit programs are focused entirely on low-income families.

During the past several years, EBT cardholders have been targeted by criminals who “skim” account information and PINs and then deplete the accounts of all funds belonging to the recipients. This problem is so endemic that even the USDA issued a policy memo on EBT card skimming prevention with tools and resources to prevent and identify the fraud,¹¹⁸ and Congress provided for reimbursement of these stolen funds for the period of October 1, 2022, to September 30, 2024.¹¹⁹

However, while other consumers have also been victimized by skimming, EBT consumers are particularly vulnerable and left with little to no recourse. Unlike other cardholders whose funds may be stolen in the same way, EBT cardholders – the lowest-income and most vulnerable consumers – do not have protections afforded to other consumers by the Electronic Funds Transfer Act or Regulation E. Even if the consumer did not lose their card, was not responsible for providing card information to the criminal, and immediately reported missing funds, they are completely out of luck. These lost funds come out of the pockets of the poorest families who cannot afford to lose a single dollar.

B. Potential remedy to address EBT card fraud.

We support legislative efforts to address gaps in the Electronic Fund Transfer Act that leave consumers unprotected. The EFTA and SNAP statute can be amended to address the specific problem of EBT card fraud by eliminating the exclusion of EBT cards from the EFTA and

¹¹⁴ U.S. Department of Agriculture, Food and Nutrition Service, “*Characteristics of SNAP Households: FY 2020 and Early Months of the Covid-19 Pandemic: Characteristics of SNAP Households*,” available at <https://www.fns.usda.gov/snap/characteristics-snap-households-fy-2020-and-early-months-covid-19-pandemic-characteristics> (last accessed September 15, 2025).

¹¹⁵ Cronquist, Kathryn and Eifles, Brett, “*Characteristics of Supplemental Nutrition Assistance Program Households: Fiscal Year 2020, Table B.4.b. Distribution of participating households by shelter-related characteristics and by State, waiver period*,” Washington: U.S. Department of Agriculture, (2022), available at <https://fns-prod.azureedge.us/sites/default/files/resource-files/Characteristics2020.pdf>; 7 C.F.R. § 273.10(c)(2)(i).

¹¹⁶ Office of Family Administration, Administration for Children and Families, “TANF Caseload Data 2022,” (August 2022) available at, <https://www.acf.hhs.gov/ofa/data/tanf-caseload-data-2022>.

¹¹⁷ U.S. Department of Health and Human Services, Office of Family Assistance, “*Characteristics and Financial Circumstances of TANF Recipients, Fiscal Year 2021*,” updated February 2023, available at <https://www.acf.hhs.gov/ofa/data/characteristics-and-financial-circumstances-tanf-recipients-fiscal-year-2021>.

¹¹⁸ U.S. Department of Agriculture, Food and Nutrition Service, *Supplemental Nutrition Assistance Program (SNAP) and Temporary Assistance for Needy Families (TANF) Electronic Benefit Transfer (EBT) Card Skimming Prevention – Tools and Resources*, (Policy memo) (October 31, 2022), available at <https://www.fns.usda.gov/snap/snap-tanf-ebt-card-skimming-prevention>.

¹¹⁹ See the Consolidated Appropriations Act (CAA) of 2023, Title IV, Section 501.

providing protection against unauthorized transfers. As a result, consumers who are impacted by EBT card theft will be able to avail themselves of the EFTA unauthorized use provision and error resolution procedures.

VIII. Problems with the Collection of Accurate Payment Fraud Data Create an Additional Barrier to Addressing Payment Fraud.

A. The problem of fragmented data collection on payment fraud.

In the United States, regulatory oversight and supervision of actors in the payments space depends on several factors including the size, type, and nature of a financial institution,¹²⁰ as well as the extent to which the activities undertaken by an institution are covered by existing law. As a result, no centralized federal agency receives or collects all data about payment fraud.¹²¹ Additionally, defrauded consumers may report fraud to the Federal Trade Commission, the FBI's internet crimes division, and/or the Consumer Financial Protection Bureau, among other local law enforcement agencies, leading to differing and incomplete snapshots of payment fraud. Although these agencies may share fraud data with each other or the general public, there is no mandate to do so.¹²²

Furthermore, financial institutions, payment processors, and payment operators are not required to report the incidents of payment fraud experienced by their customers/consumers to any federal agency. The institutions are required to file a Suspicious Activity Report (SAR) for large transactions in certain circumstances if they suspect their customer is engaged in fraudulent activity, but they are not required to report smaller fraudulent transactions or instances where their clients have been victimized by fraud.¹²³ Even with SARs mandatory reporting, the

¹²⁰ Depending on the size and activity, a financial institution engaging in payment activity could be subject to supervision by the Office of the Comptroller of the Currency, the Federal Reserve Board, the Federal Deposit Insurance Corporation, the National Credit Union Administration, and/or the Consumer Financial Protection Bureau. Otherwise, the institution could be subject to state regulatory supervision under a state bank charter or money transmitter license. Some payment stablecoin issuers will be supervised by the OCC, while others may choose to continue to be licensed by states and subject to state supervision. It is still unclear what federal agency will supervise crypto companies engaging in payments. Some payment actors may not be subject to any supervision, though they are still required to comply with all laws.

¹²¹ Of any type, including fraud through P2P apps, bank-to-bank transfers, or check fraud.

¹²² Though certain fraudulent activity is required to be reported to FinCEN, and the Federal Reserve Board will collect fraud data through FedNow. However, FinCEN does not publicly share the data it collects, and it is unclear how the Federal Reserve Board will utilize and disseminate the data it will collect for FedNow.

¹²³ "Dollar Amount Thresholds- Banks are required to file a SAR in the following circumstances: insider abuse involving any amount; transactions aggregating \$5,000 or more where a suspect can be identified; transactions aggregating \$25,000 or more regardless of potential suspects; and transactions aggregating \$5,000 or more that involve potential money laundering or violations of the BSA. It is recognized, however, that with respect to instances of possible terrorism, identity theft, and computer intrusions, the dollar thresholds for filing may not always be met. Financial institutions are encouraged to file nonetheless in appropriate situations involving these matters, based on the potential harm that such crimes can produce. Even when the dollar thresholds of the regulations are not met, financial institutions have the discretion to file a SAR and are protected by the safe harbor provided for in the statute." From FDIC "Connecting the Dots... The Importance of Timely and Effective Suspicious Activity Reports" Supervisory Insights, (Updated July 10, 2023), available at <https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin07/siwin07winter2007-article03.html#:~:text=Dollar%20Amount%20Thresholds%20%E2%80%93%20Banks%20are,and%20transactions%20aggregating%20%24%2C000%20or>.

information collected by FinCEN relies heavily on the discretion of a financial institution, whether the fraud or potential fraud is discovered/flagged by the reporting institution, and if the transaction is large enough to warrant reporting.¹²⁴

Players in the payment industry have recognized the need for fraud information sharing, and some payment operators do collect data about fraud. The Federal Reserve Board collects reports of fraud on FedNow as specified under Regulation J, Subpart C and keeps a “Negative List” of suspicious accounts that is shared with its participants.¹²⁵ The Clearing House also collects fraud reports for RTP® (their real time payments platform) and Early Warning Systems (EWS), owner of Zelle, collects reports of fraud occurring on Zelle, though it is unclear if this information is shared widely among users.¹²⁶ Even initiatives such as Sonar¹²⁷ and Beacon¹²⁸ were launched in response to increased fraud in digital payments and real-time payment systems. However, the information shared is not available to the public and may be industry or payment specific. For example, if a bad actor is flagged in one payment system (i.e. Zelle), that does not mean a financial institution will have that bad actor flagged when allowing a fraudulent wire transfer to be released.¹²⁹

The fragmentation described above prevents a clear and cohesive picture of the payment fraud landscape, actors, and trends and poses a barrier to forming effective strategies to combat fraud.

B. Potential remedies to address the problem of fragmented payment fraud data collection.

1. Interagency collaboration.

The importance of information sharing and collaboration between state and federal law enforcement agencies charged with protecting the public from fraud and other unfair, deceptive, and abusive business practices cannot be overstated. Collaboration is essential not only to identify illegal practices that harm consumers, but to facilitate a comprehensive and effective

¹²⁴ See Mansfield, Cathy, “It Takes a Thief... and a Bank: Protecting Consumers From Fraud and Scams on P2P Payment Platforms,” 57 U. Mich. J.L. Reform (2024).

¹²⁵ See Operating Circular 8: Funds Transfers through the FedNow Service, (September 21, 2022), available at <https://www.frbervices.org/binaries/content/assets/crsocms/resources/rules-regulations/operating-circular-8.pdf>.

¹²⁶ See *Faster Payments Fraud Trends and Mitigation Opportunities*, Faster Payments Council, Fraud Work Group Bulletin.01 at 5, (January 2024), available at

https://fasterpaymentscouncil.org/userfiles/2080/files/FPC%20Fraud%20Bulletin_01_01-24-2024_Final.pdf.

¹²⁷ <https://www.joinsonar.com/>, (last accessed September 15, 2025). Sonar is “an independent data consortium for sharing real-time insights into First-Party Fraud and Counterparty Risk.... By monitoring transactions across banks, merchants, fintechs, and crypto, you’re always a step ahead in detecting financial crime.”

¹²⁸ Meier, Alain “Introducing Beacon, the Anti-Fraud Network,” Plaid, (June 22, 2023), available at <https://plaid.com/blog/introducing-plaid-beacon/>. Beacon, launched by Plaid, is intended as an anti-fraud network enabling financial institutions and fintech companies to share critical fraud intelligence via API across Plaid. Members contribute by reporting instances of fraud and can use the network to detect if a specific identify has already been associated with fraud.

¹²⁹ Any private database of suspected fraud actors could be considered a “consumer reporting agency” (CRA) under the Fair Credit Reporting Act (FCRA). Early Warning Services already acknowledges it is a CRA. See CFPB, List of Consumer Reporting Companies at 28, (2023), available at https://files.consumerfinance.gov/f/documents/cfpb_consumer-reporting-companies-list_2023.pdf. As such, these databases would be subject to the file disclosure, accuracy, and dispute resolution rights under the FCRA.

strategy to stop fraudsters before they have stolen money from individuals and families. Criminals know no boundaries; they leverage technology to perpetrate their schemes quickly and are oftentimes unknown until it is too late. Staying ahead of these players requires rigorous and easy lines of communication between partners—including private attorneys and non-profit organizations—who are often the first to hear about scams on the ground.

NCLC provided many of the recommendations that follow in comments to the FTC Collaboration Act of 2021.¹³⁰ One of these recommendations is that the FTC develop a Fraud Task Force to ensure more regular information sharing and cooperation among all the various agencies that see and deal with individual pieces of the fraud landscape.

We therefore support legislation¹³¹ that encourages partnerships among various stakeholders, including regulators, industry representatives, consumer groups, and victim support groups. These kinds of task forces will not solve the problem of payment fraud, but will be an important first step to broaden information sharing.

2. Simplify fraud reporting.

Since reportfraud.ftc.gov and ic3.gov are two of the most used sites to report fraud, the FTC and the FBI should work with the CFPB, banking regulators, and state Attorneys General (AGs) and local law enforcement to simplify fraud reporting for consumers. Consumers may report fraud to many different places – the local police department, the FBI, an AG, the CFPB, or the FTC. Sometimes police refuse to take fraud reports, viewing fraud as a civil matter. Once a consumer is turned away once place, they may give up. We advise consumers to file a complaint in as many places as possible, but that is cumbersome and not always realistic. Consumers may also find that they are asked for the same information multiple times from different agencies. We urge these agencies to:

- Develop standardized complaint intake forms that can be used by many different agencies.
- Provide a range of easily accessible channels (e.g. in person, phone, e-mail, web, mobile app) for consumers to submit complaints and grievances.
- Include options to report fraud and other complaints in multiple languages.

Fraud reporting must be as simple and universal as possible to be effective.

¹³⁰ See NCLC et al., *Comments regarding the FTC Collaboration Act of 2021*, (August 14, 2023), available at https://www.nclc.org/wp-content/uploads/2023/08/FTC_AG-Fraud-Collaboration-consumer-comments-8-14-23-final13-Lauren-Saunders.pdf.

¹³¹ See, e.g. the Taskforce for Recognizing and Averting Payment Scams Act (TRAPS ACT), 2025. (S. 2019) available at <https://www.congress.gov/bills/119th/congress/senate-bill/2019/text>; Financial Services and General Government Appropriations Bill, 2024. (S. 2309), Title I. Department of the Treasury, “Financial Fraud” at 10, available at https://www.appropriations.senate.gov/imo/media/doc/fy24_fsgg_report.pdf.

3. Require fraud reporting within payment systems.

As previously mentioned, the operators of FedNow, RTP®, and Zelle already collect reports of fraud, and they should analyze those reports, follow up on patterns, and develop preventive measures if they are not already doing so.

It is critical for every entity participating in payments, such as payment providers, financial institutions, and network providers, like the Federal Reserve Board, to:

- Develop and constantly improve measures to prevent fraud in the first place;
- Detect and stop fraud as soon as possible;
- Share information about fraudulent actors;
- Build in incentives and processes for consumers to report fraud; and
- Develop and include in the system rules methods to compensate victims and correct errors wherever possible.

We especially urge the Federal Reserve Board, the operators of other wire transfer services, and other bank regulators to devote attention to bank-to-bank wire transfers. While there is a fair amount of knowledge about how consumers are defrauded into sending funds through wire transfers, no one seems to be collecting or analyzing information about the accounts into which funds are sent. Some of these questions can only be answered by the banks, bank regulators, or wire transfer operators. We understand that the Federal Reserve Board does not receive fraud reports from institutions utilizing Fedwire, though it may be exploring doing so. We do not know what fraud information is collected on other wire transfer services, such as The Clearing House's CHIPS system. NCLC provided suggestions on how the Reserve Banks and the Federal Reserve Board can build protections into Fedwire operations and impose requirements on Fedwire users to help detect fraud, prevent it from spreading, and recover money sent due to fraud or error when possible.¹³²

As previously mentioned, the Federal Reserve Banks should also explore collecting information on check fraud.

The more information law enforcement, payment system operators, and regulators have about fraud committed through these platforms, and the more that agencies work together to identify trends, the more avenues there will be for stopping fraud.

4. Require FinCEN to update the Suspicious Activity Report (SAR) to capture information about accounts that receive fraudulent funds.

FinCEN can help in the fight against payment fraud by updating the suspicious activity report (SAR) to encompass information about the accounts used to receive ill-gotten funds. The current SAR form only accommodates accounts related to the reporting institution. In fraud cases where

¹³² NCLC, *Comments regarding the Request for Information on Potential Actions to Address Payments Fraud by the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, and Federal Deposit Insurance Corporation*, at 26-31 (September 15, 2025), available at https://www.nclc.org/wp-content/uploads/2025/09/2025.09.15_Comments_Fraud-RFI-on-Payments-Fraud.pdf.

the destination account of the perpetrator is known, reporting institutions relegate the destination account to the narrative. This makes identification and aggregation of fraudulent activity more difficult for law enforcement.

When a consumer's financial institution files a SAR following an incident of payment fraud, if the payment was sent through a system that identifies the recipient (such as a wire transfer, ACH, or P2P system), the SAR should identify the recipient institution and account. Allowing accounts not domiciled at the reporting institution to be reported and designated appropriately would assist FinCEN and law enforcement in identifying, aggregating, and prioritizing fraud investigations to better protect consumers.

Since fraud schemes affect many victims at various reporting institutions, fraud often results in a hub-and-spoke relationship with one account receiving funds from many different, unrelated accounts. This typology is recognized in the FFIEC Exam Manual and should be supported at FinCEN by enhancing the SAR reporting process to include the fraud perpetrator's account at the receiving institution.

5. Ensure consumers are protected from false positives.

Although there are legal obstacles to sharing specific PII (personal identifying information) about an accountholder who may be engaging in payment fraud, this information is critical to stop criminal fraudsters from opening accounts that are then used to receive fraudulent payments. Account numbers without the accountholder's individual or business information are not as useful in preventing future fraud by that same individual or business.

At the same time, if current legal regimes are interpreted or amended to allow for this type of information sharing (including changes to the BSA or the Gramm-Leach-Bliley Act),¹³³ then innocent consumers who are negatively impacted by the sharing of this information need adequate protection. Consumers who experience an account closure, account freeze, or the inability to open a new bank account after a closure due to suspected fraud (an adverse action) based on the shared information should have protections like those already provided under the Fair Credit Reporting Act. These protections should ensure, at a minimum, that:

- Any shared information is accurate and not misleading;
- A consumer is given notice if the shared information leads to an adverse action;
- A consumer is given the opportunity to dispute the inaccuracy of any shared information and have the information be corrected if inaccurate; and

¹³³ For additional feedback on the consumer protections needed in the context of information sharing and privacy, see EPIC and NCLC, *Comments to the U.S. House Committee on Financial Services In re: Request for Feedback on Current Federal Consumer Financial Data Privacy Law and Potential Legislative Proposals*, (August 28, 2025), available at <https://epic.org/wp-content/uploads/2025/09/EPIC-NCLC-HFSC-financial-privacy-comment.pdf>.

- The entity that took the adverse action against the consumer investigates the consumer's dispute and takes any remedial action if the adverse action was based on inaccurate information.

In other words, Congress and regulators should encourage information sharing to prevent and stop fraud, but only when adequate guardrails are in place to address false positives and provide relief when innocent consumers are harmed by the false positives.

As discussed in more detail below, impacted consumers should have an avenue for disputing account closures and freezes through the EFTA's error resolution procedures.

IX. Challenges with Account Freezes, Closures, and Holds Due to Fraud Lead to Debanking Consumers.

In recent years, many consumers have raised concerns about bank account closures and/or freezes that seem to occur without any sudden change of behavior by the consumer or in response to a fraud dispute by the consumer (when the consumer reports that some unauthorized use has occurred in their account). Some consumers have also reported that even when a financial institution temporarily credits an account for a fund transfer that a consumer has disputed as unauthorized, the financial institution will then refreeze that amount or the entire account within hours after the recredit. Consumers report frustration and uncertainty tied to account closures and freezes— primarily due to the lack of information regarding why the closure or freeze occurred and the inability to access funds in a timely manner.

The number of consumers who have complained about checking and savings account closures to the CFPB more than doubled since 2017.¹³⁴ In 2022, the CFPB ordered Wells Fargo to pay \$160 million to over one million people for improperly freezing or closing bank accounts from 2011 to 2016 when it “believed that a fraudulent deposit had been made into a consumer deposit account based largely on an automated fraud detection system.”¹³⁵

There have also been stories featured by reporters detailing the devastating impact sudden account closures and freezes can have on consumers, especially when they are deprived access to their funds, are not provided with any information about the reason for the institution's actions, and are not provided an opportunity to address any perceived risk.¹³⁶

¹³⁴ Consumer Financial Protection Bureau, Consumer Complaint Database, trends data for complaints received due to checking or savings account closure, https://www.consumerfinance.gov/data-research/consumer-complaints/search/?chartType=line&dateInterval=Month&dateRange=All&date_received_max=2024-01-27&date_received_min=2011-12-01&has_narrative=true&issue=Closing%20an%20account%E2%80%A2Company%20closed%20your%20account&lens=Product&product=Checking%20or%20savings%20account&searchField=all&subLens=sub_product&tab=Trends, (last visited February 20, 2024).

¹³⁵ *In re. Wells Fargo Bank, N.A.*, CFPB No. 2022-CFPB-0011 (December 20, 2022) (consent order), available at https://files.consumerfinance.gov/f/documents/cfpb_wells-fargo-na-2022_consent-order_2022-12.pdf.

¹³⁶ Barnard, Tara Siegel and Lieber, Ron, “Banks Are Closing Customer Accounts, With Little Explanation,” *New York Times*, (April 8, 2023), available at https://www.nytimes.com/2023/04/08/your-money/bank-account-suspicious-activity.html?unlocked_article_code=1.QU0.szRm.kfoZROdD7-O6&smid=url-share; Kessler, Carson, “A Banking App Has Been Suddenly Closing Accounts, Sometimes Not Returning Customers’ Money,” *ProPublica*, (July 6, 2021), available at <https://www.propublica.org/article/chime>; McGreevy, Patrick, “Bank of America must

One of the reasons for the increase in account closures and freezes has to do with the increased adoption of tools utilized by financial institutions to combat payment fraud and detect suspicious activity, including adoption of artificial intelligence (AI) and machine learning technologies. Fraud vigilance is critical, and new technologies can play an important role. However, these tools may harm innocent consumers if not utilized properly and if institutions do not have clear procedures and timelines in place to restore access to funds that are improperly frozen.

A. Overaggressive fraud algorithms can shut out innocent consumers from access to their bank accounts and funds, and overly broad BSA programs prevent these consumers from understanding why those actions were taken.

Financial institutions have an obligation under the BSA to ensure that they maintain and follow internal ongoing Customer Due Diligence (CDD) programs and policies. The CDD program's policies must allow the institution to understand "the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and [c]onducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information."¹³⁷

Because of the CDD obligation and the ongoing problem of payment fraud, sometimes the appropriate response by an institution that suspects its customer is engaging in fraudulent or other illicit activity is to freeze a transaction or close an account that is being used to receive fraudulent funds before the funds are gone and more consumers can be defrauded. But sometimes financial institutions get it wrong, especially when automated tools are used. No law requires a financial institution to take these actions; it is up to the risk tolerance of the company and the internal policies set in place by the company. The only required response to potential fraud a company may need to undertake under BSA/AML law is to file a SAR if the transaction is large enough to meet the threshold reporting requirements and update their customer risk profile.¹³⁸

According to the Bank Policy Institute, "a sample of the largest banks reviewed approximately 16 million alerts, filed over 640,000 SARs, and received feedback from law enforcement on a median of 4% of those SARs. Ultimately, this means that 90-95% of the individuals that banks report on were likely innocent."¹³⁹ As these numbers demonstrate, even activity that leads to the filing of a SAR may ultimately not warrant an account freeze or closure.

provide more proof of fraud before freezing EDD accounts, court orders," Los Angeles Times, (June 1, 2021), available at <https://www.latimes.com/california/story/2021-06-01/bank-of-america-ordered-to-unfreeze-unemployment-benefit-cards-in-california>; KCAL News, "Bank Of America Freezes EDD Accounts Of Nearly 350,000 Unemployed Californians For Suspected Fraud," (October 29, 2020), available at <https://www.cbsnews.com/losangeles/news/bank-of-america-freezes-edd-accounts-of-nearly-350000-unemployed-californians-for-suspected-fraud/>.

¹³⁷ 31 C.F.R. § 1020.210(a)(2)(v);(b)(2)(v).

¹³⁸ Financial Crimes Enforcement Network, *Customer Due Diligence Requirements for Financial Institutions*, Final Rule, 81 Fed. Reg. 29398 (May 11, 2016); 31 C.F.R. 1020.210(b)(i); Office of the Comptroller of the Currency, *Bank Secrecy Act (BSA)*, available at <https://www.occ.treas.gov/topics/supervision-and-examination/bsa/index-bsa.html/>.

¹³⁹ Bank Policy Institute, "The Truth About Suspicious Activity Reports," (September 22, 2020), available at

To compound matters, many financial institutions believe that if an account was closed or frozen and a SAR was filed, they are not allowed to disclose the reason why the account was closed or frozen, because it would lead to the assumption that a SAR was filed. As a result, consumers are not told why their account is closed or funds are frozen, or they are given the run-around. Many consumers have reported that financial institutions reply that they cannot disclose any information as to why the account was closed or frozen. Yet financial institutions are only prohibited from disclosing the existence of the SAR, not responding to consumer concerns that their account was frozen or closed improperly.

The impact of sudden account closures in response to potential fraud on innocent consumers cannot be overstated. Often, the most vulnerable people have been denied access to their money, rendering them unable to eat or pay rent. Some impact on innocent individuals may be impossible to avoid, as banks may need to act quickly on imperfect information. But that is why it is imperative to have procedures in place to enable people to dispute account freezes and closures and get their money back as soon as possible.

If people cannot access the money they need based on red flags triggered by automated fraud tracking systems, then they need a timely solution, not another obstacle. Yet that is what occurs; consumers face obstacles upon obstacles. When a consumer complains about an account closure or freeze, the complaint is often not followed by a reasonable investigation by the financial institution that includes a discussion with the consumer or that provides any clear timeline to unfreeze their money.

NCLC has assisted many impacted consumers with complaints to the OCC, Treasury (when an impacted account was through the Direct Express program), or by leveraging connections within large financial institutions to look into an account and resolve the issue. However, this is not a sustainable solution for all impacted consumers. Policies need to change. Crude AML/CFT compliance policies and overly broad fraud responses can shut consumers out of our banking system.

The EFTA has clear error resolution timelines and procedures, and those should be used when consumers cannot access their funds. When a consumer is unable to make an electronic withdrawal or transfer because of an account closure or freeze based on suspected fraud, that action should be viewed as an error – an incorrect transfer of zero instead of the requested amount – triggering the error resolution rights, duties, timelines, and investigation procedures of the EFTA. The EFTA's error resolution procedures can also be triggered by the consumer's request for information about a failed EFT, which is another enumerated error under the EFTA.¹⁴⁰ However, financial institutions and payment apps seem to believe the EFTA does not apply in this situation.

<https://bpi.com/the-truth-about-suspicious-activity-reports/> (citing, Bank Pol'y Inst., *Getting to Effectiveness—Report on U.S. Financial Institution Resources Devoted to BSA/AML & Sanctions Compliance*, (October 29, 2018) available at https://bpi.com/wp-content/uploads/2018/10/BPI_AML_Sanctions_Study_vF.pdf).

¹⁴⁰ 15 U.S.C. § 1693f(f)(6).

B. Potential remedies to address improper freezes or account closures due to the use of automated fraud detection.

The problem with account closures and freezes could be addressed by rulemaking or guidance from the CFPB, though that is not necessary. Regulators should interpret the EFTA's error resolution procedures to apply to disputes from consumers when EFTs fail because of an account freeze or closure. The EFTA's error resolution procedures allow financial institutions to continue using automated fraud detection systems while ensuring that there are procedures in place for resolving disputes in a reasonable time and give consumers remedies when those systems get it wrong. This would ensure a consumer receives information about why their account was frozen or closed and get more timely access to their funds if the bank was in error.

Even apart from the EFTA, the CFPB and bank regulators should also provide guidance to financial institutions about the importance of having clear procedures to enable consumers to quickly regain access to their funds when they are frozen due to concerns of suspicious activity, provide guidance as to the timeliness of returning an accountholder's funds after account closure, and specify that failing to have clear procedures and provide timely return of any funds may constitute an unfair, deceptive, or abusive business practice.

Bank regulators, along with FinCEN, should provide guidance to financial institutions about what information they may and should provide to accountholders regarding freezes and account closures while still complying with the BSA. For example, they could clarify in an FAQ that, while financial institutions are not allowed to disclose that a SAR was filed, they are allowed to describe the specific activities that raised concerns, giving the consumer an opportunity to respond and appeal a decision that was made in error, or based on false assumptions or false red flags. They should also clarify that if a SAR does not lead to criminal prosecution or involvement by law enforcement for suspected money laundering/financing of terrorism activity, then a financial institution should not automatically take derisking measures and close the account based solely on the filing of a SAR, but the institution should instead take a measured, case-by-case, risk-based approach.

Finally, regulators should investigate the reasons that deposit accounts are closed or frozen and develop a strategy to minimize the number of account closures for innocent consumers.

X. Fraud Traverses Many Industries and Sectors, and the Federal Government Must Take a Holistic Approach to Combatting Fraud.

A. Criminal Fraudsters rely heavily on text messages to initiate fraud schemes.

Calls and text messages are a significant and increasing contact method for fraud. In 2022, victims reported losses of over \$1.1 billion from phone and text message-based scams.¹⁴¹ Reported losses have been increasing steadily and substantially to over \$1.4 billion in 2024.¹⁴²

¹⁴¹ FTC Consumer Sentinel Network, Fraud Reports by Contact Method, Reports and Amount Lost by Contact Method, Year: 2021, (updated Feb. 22, 2022), available at <https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts>.

¹⁴² [Consumer Sentinel Network Data Book 2024](#), at pg. 12.

Scammers are attracted to calls and texts because they can use them inexpensively and anonymously through complicit service providers that know they are transmitting scam calls to consumers. These providers make money connecting scammers to their victims, and given the steadily increasing losses from phone and text scams, it is clear that existing laws and regulations do not have a sufficient deterrent effect.

Increased collaboration among the prudential regulators, the Federal Communications Commission (FCC), and other stakeholders could help prevent payments fraud resulting from imposter scams. Imposter scams occur when a criminal fraudster pretends to be a government agency, financial institution, or legitimate business. The criminal then contacts a consumer to alert them to a fake and urgent problem and attempts to persuade them to transfer their money under these false pretenses.¹⁴³ Imposter scams are a rapidly intensifying problem that disproportionately impacts older adults. Indeed, “combined losses reported by older adults who lost more than \$100,000 increased eight-fold, from \$55 million in 2020 to \$445 million in 2024.”¹⁴⁴

Financial institutions as well as consumers are harmed by these scams, which often start as robocalls or texts that appear to be from banks, with text messages like this:

Wells Fargo Bank Fraud Alert:
Did you attempt a purchase at
Walmart for \$1,263.89? Reply
YES or NO

A reply to the text will precipitate a call from the (fake) fraud department. Victims say they thought the bank was helping them get their money back. Instead, money was transferred out of their account. This scam’s median reported loss was \$3,000. The FTC announced that in

2023, these scams accounted for \$330 million in reported losses.¹⁴⁵

B. Recommendations to address scams initiated by text.

NCLC has previously urged the OCC to address imposter scams and the resulting payments fraud by encouraging or requiring banks to employ safe texting protocols, which allow consumers to easily differentiate between legitimate communications from their financial institutions and dangerous imposter scam texts.¹⁴⁶ Additional collaboration with the FCC to identify and promulgate measures to address the role of scam calls and texts in imposter scams will help to detect and prevent payments fraud.

Additionally, prudential regulators should consider collaboration with law enforcement agencies and state attorneys general and regulators to prosecute companies that facilitate and profit from

¹⁴³ See “*FTC Data Show a More Than Four-Fold Increase in Reports of Impersonation Scammers Stealing Tens and Even Hundreds of Thousands from Older Adults*,” (August 7, 2025), available at: <https://www.ftc.gov/news-events/news/press-releases/2025/08/ftc-data-show-more-four-fold-increase-reports-impersonation-scammers-stealing-tens-even-hundreds>.

¹⁴⁴ *Id.*

¹⁴⁵ FTC, “*New FTC Data Analysis Shows Bank Impersonation is Most-Reported Text Message Scam*,” (June 8, 2023), available at <https://www.ftc.gov/news-events/news/press-releases/2023/06/new-ftc-data-analysis-shows-bank-impersonation-most-reported-text-message-scam>.

¹⁴⁶ See NCLC’s letter to the OCC available at: https://www.nclc.org/wp-content/uploads/2024/10/2024.03.29_Letter_OCC-and-Texts.pdf

imposter scams and other fraud. For example, the Social Security Administration's (SSA) Office of the Inspector General and the Department of Justice partnered with several law enforcement agencies, the FCC, and the Federal Trade Commission to bring enforcement actions against several communications providers that knowingly transmitted scam calls impersonating the SSA.¹⁴⁷

Congress should also pass legislation and work with the FCC to address fraud facilitated by texts and calls.¹⁴⁸ Some of these include:

- Requiring a bond for transmitters of phone calls and texts.¹⁴⁹ This will force providers to either post a substantial sum or convince a third-party bond company that it is a legitimate company that does not intend to transmit fraudulent calls to U.S. consumers.
- Fixing any uncertainty as to whether the FCC has a legal pathway to assess civil penalties by restoring the FCC's enforcement ability. Congress should specifically authorize the FCC to file actions for civil penalties in federal district courts.
- Requiring rigorous know-your-customer and know-your-traffic procedures that force carriers to vet callers and calls that transit their network.
- Requiring record-keeping for call originators to ensure that information about callers is available for government or private enforcement efforts.
- Requiring carriers to investigate call traffic that displays suspicious characteristics, like a high percentage of short-duration calls and other indicia of fraud.
- Adopting federal regulations for phone number resellers to address phone number rotation schemes that allow callers to undermine the goals of the STIR/SHAKEN framework.¹⁵⁰
- Strengthening the Telephone Consumer Protection Act (TCPA) to encourage robust enforcement against scam callers and those who facilitate fraud by:
 - including an explicit cause of action for assisting and facilitating callers who violate the TCPA;
 - amending the definition of "telephone solicitation" and telemarketing in the TCPA and regulations to cover scam calls, for instance, by explicitly extending existing definitions to cover calls that attempt to defraud, cause harm, or wrongfully obtain anything of value;

¹⁴⁷ Office of the Inspector General, Social Security Administration, "Civil Action to Prevent Social Security Scam Calls from Reaching Consumers," available at <https://oig.ssa.gov/scam-alerts/2025-07-17-civil-action-to-prevent-social-security-scam-calls-from-reaching-consumers/> (last accessed September 16, 2025).

¹⁴⁸ See NCLC, *Letter to the Joint Economic Committee regarding the problems caused by scam calls and texts*, (June 16, 2025), available at <https://www.nclc.org/wp-content/uploads/2025/07/Email-to-JEC-6-16-25.pdf>.

¹⁴⁹ VoIP providers should be required to obtain a bond from a third-party and show proof of the bond before they can obtain the certifications necessary to sign calls under the STIR/SHAKEN framework. Bond amounts could ensure that there are funds available to satisfy judgements obtained in government or private enforcement actions related to illegal calls. Bond issuers would have an economic incentive to vet bond applicants thoroughly to make sure they are identifiable and unlikely to transmit illegal calls that would result in damages that the bond issuer would have to pay out of the bond amount. Originating carriers would risk losing their bond if they provided false STIR/SHAKEN attestations or allow unknown entities to place calls through their network.

¹⁵⁰ Phone number resellers who do not keep records that identify the end user of a phone number should be held liable for any losses caused by calls using the phone number. And a fee for short term use of phone numbers should be instituted to make it deter the purchase temporary phone numbers for use in rotation schemes by making it economically infeasible.

- extending the existing cause of action for violation of the TCPA's do-not-call regulations to allow individuals to bring a suit after receiving one violative call;
- creating a private cause of action for violations of the technical and procedural restrictions in the TCPA; and
- allowing for recovery of attorney's fees for a prevailing plaintiff in a TCPA suit.
- Strengthening the Telemarketing Sales Rule (TSR) to expand enforcement by:
 - Reducing or removing the requirement of \$50,000 in individual damages for private suits under the TSR;
 - expanding the definition of "telemarketing" in the TSR to cover scam calls, for instance, by explicitly extending existing definitions to cover calls that attempt to defraud, cause harm, or wrongfully obtain anything of value; and
 - specifying that short-term use of telephone numbers in rotation schemes is a deceptive telemarketing practice.

XI. Fraud Prevention Education Is Necessary in the Fight Against Fraud, But It Will Not Solve the Problem.

Although consumer and business education is important, it alone will not solve the problem of payment fraud. Criminal fraudsters have extraordinary creativity;¹⁵¹ they are constantly developing ways to steal people's money by setting up increasingly sophisticated schemes to obtain access to accounts or to fraudulently induce consumers into payment transactions.¹⁵²

¹⁵¹ For examples of the types of scams utilized by robocalls and scam texts, see NCLC, EPIC report *Scam Robocalls: Telecom Providers Profit*, at 6-10 (June 2022), available at <https://www.nclc.org/wp-content/uploads/2023/02/Robocall-Rpt-23.pdf>; see also Testimony of Margot Saunders, NCLC "Protecting Americans from Robocalls," Hearing Before the U.S. Senate Committee on Commerce, Science & Transportation, (October 24, 2023), available at <https://www.nclc.org/wp-content/uploads/2023/10/Testimony-of-NCLC-on-Robocalls-2023.pdf>.

¹⁵² See the scam warning below which also involves impersonation of law enforcement.

This Fake App Takes the Cake

This recent scam is impressively complex. The cybercriminals start by impersonating law enforcement officers. They contact you, claiming that your bank account may have been involved in financial fraud. You're then asked to download a mobile app to help them investigate further. If you download the app, the cybercriminal walks you through the steps to set this scam in motion.

First, you are given a case number. When you search for that number in the app, you'll find legal-looking documents with your name on them. These documents make the scam feel more legitimate. Once your guard is down, the app asks you to select your bank from a list and then enter your account number and other personal information.

As soon as consumers receive notice and information about one type of scam, the criminal fraudsters will develop new avenues and methods to defraud them. As a result, we recommend in-app and real-time education by payment providers and financial institutions, as well as social media and telecommunications providers. For example, simply requiring “confirmation of payee” prompts and pop-ups with questions about transactions and red flags may prevent consumers from sending payment to a criminal fraudster.

Consumers and businesses should also receive broader education about cybersecurity instead of just scams and fraud. Better education about internet safety, phishing, vishing, ransomware, and business email compromise would also reduce the amount of account takeovers and fraud schemes that lead to monetary loss from payments fraud.

With respect to check fraud, we support consumer education about safer ways to make payments.¹⁵³ For example, as we described in our comments to the Treasury Department’s Request for Information on Modernizing Payments,¹⁵⁴ the goal of reducing the number of paper

The most clever part of this scam is what the app does in the background. When you first install the app, it blocks all incoming calls and text messages. That way, you won’t be alerted if your bank attempts to contact you about unusual behavior on your account. If all goes as planned, the cybercriminals will steal your money and sensitive information before you know what happened.

No matter how advanced the app is, you can stay safe from scams like this by following the tips below.

- Only download apps from trusted publishers. Anyone can publish an app on official app stores or sites—including cybercriminals.
- Be cautious of scare tactics that play with your emotions. Cyberattacks are designed to catch you off guard and trigger you to reveal sensitive information.
- If you’re contacted by someone claiming to be in a position of authority, like law enforcement, ask them to confirm their identity. Real officials will understand your concerns and can provide information that doesn’t require you to download an app.

The KnowBe4 Security Team
KnowBe4.com

¹⁵³ See, e.g., AARP, “Should You Stop Using Paper Checks?” (August 14, 2023), available at <https://www.aarp.org/money/scams-fraud/prevent-stolen-checks-mail-theft/>.

¹⁵⁴ NCLC, *Comments to the Department of Treasury’s Request for Information on Modernizing Payments*, (June 30, 2025), available at https://www.nclc.org/wp-content/uploads/2025/07/2025.06.30_Comments_Modernizing-Payments-To-and-From-Americas-Bank-Account.pdf.

checks sent by and to the federal government is a worthy one. We support outreach to identify the reasons that people use paper checks, to address those reasons, and to encourage people to send and receive money through safer electronic payments. However, we oppose simply ending all use of checks to and from the federal government on a given date, which will only harm consumers.

At the same time, the fear of fraud in electronic payments is one of the reasons that people use checks today. Even if electronic payments are safer than checks (we do not know if that is actually true on a percentage basis, especially if you include fraudulently induced payments), reports of fraud on electronic payment platforms and the lack of consumer remedies make many people hesitant to use those platforms. Thus, we need to both reduce fraud in electronic payments and improve remedies for consumers as part of the transition away from checks.

We also support consumer education about safer ways to pay by check, such as the use of permanent ink and taking mail directly to the post office. AARP has put out materials on that topic.¹⁵⁵ The Agencies and financial institutions can educate consumers on these methods – which will also serve the goal of making people aware of check washing and encourage the use of electronic payments.

Finally, any education that is provided to consumers (including in-app pop-ups or notifications) should be done in a language that is chosen by the consumer and with considerations for individuals with disabilities. Individuals with limited English proficiency or disabilities are often targeted by criminal fraudsters and are the most vulnerable to fraud schemes that take advantage of the lack of access to information that is available in a form that can be understood.

XII. Conclusion

Payment fraud is a pervasive problem impacting U.S. consumers, especially those most vulnerable to the loss of income caused by unauthorized and fraudulently induced transactions. However, Congress can take steps to address these problems by utilizing a holistic approach to the problems caused by fraud and scams instead of just relying on consumer education and information dissemination.

With any questions, please contact Carla Sanchez-Adams, Senior Attorney at the National Consumer Law Center, at csanchezadams@nclc.org.

Thank you for the opportunity to provide this statement for the record.

Yours very truly,

National Consumer Law Center (on behalf of its low-income clients)

¹⁵⁵ See AARP, “6 Ways You Can Thwart Check Washers,” (March 2, 2023), available at <https://www.aarp.org/money/scams-fraud/stop-check-washers/>.

Chairman MEUSER. Thank you very much for your testimony.

We will now turn to member questions. The chair recognizes himself for 5 minutes.

Fraud and scams are not new concepts. I am extremely concerned by how rampant—as we all are—it has become in recent years.

Ms. Griffin, I would like to start with you. Can you briefly explain the difference between fraud and a scam and then elaborate—when you mentioned that fraud is a national security crisis, who is behind the scams? Who is behind the fraud? Many think it is lone actors. Others think, as you are expressing, it is criminal networks. If you could expand, please.

Ms. GRIFFIN. Yes, absolutely.

Within the financial services ecosystem, a fraud occurs when the customer has no knowledge or participation in the transaction. So, if you buy a coffee on the street here in DC and simultaneously your card is used to buy a computer in Texas, your financial institution says, “Hey, something is going on here that is not right,” but you had no knowledge of that transaction.

In a scam, you have, perhaps, met someone online; you received a phone call from someone you believe is the Federal Bureau of Investigation (FBI) asking you to move funds. You authorize that transaction to your financial institution and are part of the process. In that case, the financial institution has very different sets of information about what is happening in that transaction because you have authorized it.

You ask about who is behind this. The “Annual Threat Assessment of the U.S. Intelligence Community” has identified these scams—authorized transactions—as part of a nexus of criminal activity threatening the United States perpetuated by transnational criminal organizations and state-affiliated groups that also engage in human trafficking, drug trafficking, weapons and human smuggling.

North Korean hackers, Mexican cartels, Russian crime syndicates, and triad gangs affiliated with the Chinese Communist Party (CCP) are among the U.S. adversaries that are benefiting from these crimes.

We also know that they are using human trafficking victims in some places to commit those crimes. Scam compounds in Southeast Asia may have as many as 400,000 enslaved people forced to commit those scams against U.S. and other countries’ citizens.

Chairman MEUSER. Well, thank you. That is quite compelling.

Mr. Bednowitz, what are some of the explanations for the rise in financial fraud and scams? You mentioned it is a 33-percent increase, I think you said, over a 2-year period. I really appreciate you saying these are not just statistics; these are people that are truly being seriously victimized.

If you would, please.

Mr. BEDNOWITZ. Yes. Thank you for the question, Chairman.

There are three primary drivers of the increase in scams and fraud over time.

Chairman MEUSER. Lean into the mic a little bit.

Mr. BEDNOWITZ. Oh, sorry.

There are three primary drivers of the increase in scams and fraud over time: the increase in data breaches, the industrialization of fraud, and the rise of AI.

Data breaches have tripled since 2020, and that means there is a plethora—this is according to the Interstate Technology & Regulatory Council (ITRC) and our own data. What that means is, there are now billions and billions of pieces of personal information that are exposed on the dark web that criminals can use to target people—to target them with compelling messages from their banks, target them with spoofed numbers. That information is very critical.

Then you take that—as Ms. Griffin said, it is no longer an individual in a basement somewhere. You have criminal organizations across the world that are professional, that have large staffs, at times human-trafficked themselves, that are doing this and targeting victims day-in and day-out.

Those two on their own are enough to drive the growth, but then you take AI into it. I said AI was a double-edged sword. In the hands of these organizations—

Chairman MEUSER. Right.

Mr. BEDNOWITZ [continuing]. you know, what would have taken more time and cost to take that information that is out there in the dark web and combine it with information from social media and public internet, would be harder—that has become easier and easier, so that no longer do we have the days of the Nigerian prince scam with all of the spelling errors—

Chairman MEUSER. Right.

Mr. BEDNOWITZ [continuing]. but, instead, you have emails that look like they are from your bank, that have your account number in there, that have your name—

Chairman MEUSER. Right. Thank you. Great answers.

Mr. BENDA, relatively quickly, the Office of Scam and Fraud Prevention you brought up. There are a lot of discrepancies, whether it is \$12 billion, \$16 billion of loss from these scammers and fraud experts. Talk about that, how important that would be, to interconnect government agencies with them.

Mr. BENDA. Sure. I think the challenge we have—we have heard that the numbers that Americans are experiencing scams could be \$100 billion, and yet you have to ask yourself the question, who is in charge of scam and fraud prevention in the U.S. Government? Is it the Treasury Department? Is it Department of Justice? Is it Department of Commerce? We have no central point to report these.

In fact, consumers are confused as to where they should even report a scam or fraud. Should they report to the FBI? Should they report to the CFPB? Should they report to FTC and others?

So having a central place where we could report this information, that could be acted upon, to actually take action for the consumer—

Chairman MEUSER. My apologies. We will have to finish this later.

Mr. BENDA [continuing]. would be helpful.

Chairman MEUSER. My time has expired.

We will now turn to the gentleman from California, Mr. Liccardo, for 5 minutes.

Mr. LICCARDO. Thank you, Mr. Chair.

Thank you, each one of you, for your testimony.

I wanted to ask one question and ask for hopefully the feedback of each of you, if we can get it all done in 5 minutes. Let me describe the basis of the question.

We have been very active in this committee in attempting to set up rules to govern cryptocurrency and that is long overdue. I think many in the industry would agree that this is an area that needs some settled regulation rather than regulation by litigation or other approaches that have been taken in the past.

We know that trillions of dollars are transacted in centralized exchanges and decentralized protocols every year. That number is increasing rapidly and with that quantity of exchange, obviously, to the extent that particularly it is happening off of decentralized exchanges, there is increasing opportunity for fraud and for theft, as well as money laundering and other kinds of criminal activity.

We have recently in the House of Representatives passed a bill, the CLARITY Act, that governs what happens on centralized exchanges and perfectly or imperfectly, it has established know-your-customer requirements, anti-money-laundering requirements, other rules to establish centralized exchanges.

We know, increasingly, the activity is moving from centralized to decentralized, to decentralized finance (DeFi) protocols and because of pseudonym anonymity, the person on one end of the transaction does not actually know the identity of the person at the other end of the transaction. If they try to get a subpoena or they call the FBI to say, "I was defrauded," they cannot even find out who was doing it.

So the question is, what do we do about DeFi? That was not addressed in the bill that passed through the House.

I am interested, Ms. Sanchez-Adams, do you have any particular views?

Ms. SANCHEZ-ADAMS. Yes. As I mentioned in my testimony, I think that, regardless of the market regulation and structure of the bill, you have to protect consumers.

So, if you update or clarify—the CFPB can do it through guidance, or you all can do it through legislation—that the EFTA applies to crypto transactions, then those platforms will be held responsible and liable when consumers are defrauded, especially if you also update it to include fraudulently induced transactions.

Mr. LICCARDO. If it is off a platform, what do you do then?

Ms. SANCHEZ-ADAMS. I mean, you mean if it is, like, from an unhosted wallet?

Mr. LICCARDO. That is right.

Ms. SANCHEZ-ADAMS. Right. So, I mean, you can—I think that there are problems with crypto and with the technology aside from that, which I am happy to talk about at another point in time, but I think you still hold them liable. They are the party or the entity that is receiving the fraudulent fund.

If they are—unfortunately, it would be like I am acting in cash, and I am transacting in cash, right? So, if I have an unhosted wallet that is being used to pay somebody else who has an unhosted

wallet, it is like I am giving them cash and so they cannot be regulated the same way as a bank could be regulated, but they are still subject to criminal fraud.

Mr. LICCARDO. Thank you.

Ms. Griffin?

Ms. GRIFFIN. Thank you for question. The forthcoming report will have a number of recommendations related to this, one of which will include establishing parity of law enforcement powers across money movement, including the civil forfeiture of digital assets.

So some things about treating digital assets as cash for purposes of the civil forfeiture of fungible property; clarifying U.S. Secret Service authorities regarding those asset transactions—essentially, how do we empower our law enforcement to be able to go after when crypto is involved in the transaction.

I think the other element of this that has come up quite a bit in the task force deliberations is also related to the risks posed by crypto ATMs—ATMs that are placed in community stores, in nursing homes, in retirement homes, and where people are directed to put their hard-earned cash into those ATMs for the purposes of sending to criminals. That is an area where we think there is a greater need for you all to be investigating.

Mr. LICCARDO. Thank you.

Mr. Bednowitz, you might have the last word.

Mr. BEDNOWITZ. Yes, so thank you for the question, and I will be very brief.

I think, from our standpoint, I go back to what I said; I think awareness is very, very important. Consumers are not aware of the incredible risk that crypto poses. Crypto is at the heart of a lot of different scams, because people get excited about the potential returns, and they do not know when they send crypto to an individual, what risks they are opening themselves up to.

So making people more aware of the risks of crypto and that they should be much more thoughtful of when they are putting cash into crypto and where they do that is very, very critical to combating this issue.

Mr. LICCARDO. At the very least, we should be making them aware if they are on a DeFi protocol as opposed to a centralized exchange with those kinds of—

Mr. BEDNOWITZ. A hundred percent.

Mr. LICCARDO. Thank you very much for your testimony.

Thank you. I yield.

Chairman MEUSER. The gentleman yields.

The gentleman from Arkansas, Chairman Hill, who is our chair of our full committee, is now recognized for 5 minutes.

Chairman HILL. Thank you, Chairman.

Again, thanks to the panel. Great panel, good discussion.

I noted in my opening statement that our family was hit with washed checks from the Postal Service, and—really offensive. I want to credit my bank for finding it and recognizing the fraud and stopping it and helping work with the FBI and the local police to put the people in jail, which I was happy to do, but there are millions of people around the country that is not happening to. So this is such an important hearing.

Mr. Benda, I want to start with you and thanks for the ABA taking a keen interest in this.

All the comments I have heard are 100 percent true; there is just not a way to get at this. It is a whack-a-mole situation, and we do not have enough mole whackers working on it.

One of the things noted was, you said maybe \$100 billion of losses and one of my complaints is, we cannot measure or tackle things we cannot see. I have argued that the bank call report should break fraud losses out of other expenses and make it its own line item.

Would you support that, Mr. Benda?

Mr. BENDA. I think it is important for us to track fraud and scam losses in a consolidated manner. That would be one thing we would be open to looking at doing.

Chairman HILL. Good. Thank you.

Also, this all-of-the-above law enforcement effort that it takes—and all of you have kind of touched on that in your different remarks in answer to questions.

I went to Tyler, Texas, to look at the Tyler law enforcement center that the State of Texas has set up there to combat debit fraud—so, focused on debit skimming mostly at fuel pumps, operated by cartel-related gangs across Texas. Millions of dollars are lost per month. The card issuers are the eaters of those losses, not the merchants, generally.

What should we ask merchants to do in terms of 24-hour, 7-day-a-week, microscopic telecommunications pump point-of-sale fraud? You mentioned ATMs, a similar issue to prevent skimming.

Who wants to tackle that question?

Ms. Griffin, do you want to tackle that?

Ms. GRIFFIN. I think the only thing I will say is, we have a number of members in the task force, I know, that have been working on this issue, both related to EBT cards, as Ms. Sanchez-Adams brought up, as well as other types of transactions.

There are increasing and emerging technologies they can use at the point-of-sale devices to detect when a skimming device has been put there—

Chairman HILL. Yes.

Ms. GRIFFIN [continuing]. and more investment in that is needed.

Chairman HILL. The technology I saw is smaller than my little fingernail. It is inserted in the skimmer, both at point-of-sale at retail and at a gas pump and it is downloaded by Bluetooth to the criminal who just walks by the pumps on a regular retrieval basis.

This is not your grandmother's fraud, like you are all making the comments. This is super-sophisticated.

Attorney General Tim Griffin in my State has set up a Financial Fraud Task Force to bring all the forces together in Arkansas to combat this—text, phone, mail, check, the whole effort. So I really commend him for that.

Ms. Griffin, I wonder what your view is of how those stakeholders should try to work together on a national basis to do best practices.

In my example in Arkansas, tens of thousands of dollars are missing: \$1.5 million out of my post office just in my little neigh-

borhood was the publicly reported number. We have one postal inspector for the State of Arkansas, 3.4 million people.

So can you comment on the role of the FBI, the U.S. Postal Service, and other law enforcement?

Thank you, Ms. Griffin. Please.

Ms. GRIFFIN. Yes. Thank you.

First of all, those agencies were all very active at our table. Lots of dedicated leaders focus on this and one thing that we heard quite often is that the collaboration around scams is a side-of-the-desk activity. There is not a directive from the top that anti-scam activity is a leading priority for law enforcement.

One of the actions that we believe can be facilitated by naming scams as a national priority to mount a coordinated response is to direct law enforcement to create greater resources toward those kinds of collaborations, because, as you rightly mention, they will yield benefits.

Chairman HILL. Yes.

It is a cross-Congress problem. I mean, we do not control the FTC on this committee, and yet the FTC and the Federal Communications Commission (FCC) should be very involved here due to the transmission means that you have all addressed, like in telecommunication-based scams, which is the fastest-growing, the most accurate. You have all testified to that. So I think we have to link the financial services industry with the transmission capabilities, which is mail and telephone and text and internet.

So I want to thank the panel.

Mr. Meuser, thank you for a great hearing, and I yield back.

Chairman MEUSER. The chairman yields back.

The gentleman from Texas, Mr. Green, who is the ranking member of Oversight and Investigations, is now recognized for 5 minutes.

Mr. GREEN. Thank you, Mr. Chairman.

And, again, I thank the witnesses for appearing.

Let me start with a basic premise, and this premise is that consumers need all of the help they can get from whatever agencies are available to them, including the Consumer Financial Protection Bureau, which is currently under assault.

Currently, an effort is afoot to remove some 1,500 of the personnel from the CFPB. This would be tantamount to removing about 90 percent of the staff. Consumers need all the help they can get, at a time when this President is eviscerating the Consumer Financial Protection Bureau.

Now, Ms. Sanchez, you made a comment earlier—Sanchez-Adams—about the CFPB. Some of what my colleagues, my friends, as witnesses, are calling to our attention are things that the CFPB could be associated with. If needed, we could expand what the CFPB can do. Someone said, we need a central point of contact for consumers. Well, that sounds like a Consumer Financial Protection Bureau, which is being eviscerated.

This hearing is quite amazing to me. We want to help consumers, by some standards—not mine—by eviscerating the agency that helps consumers.

Ms. Sanchez-Adams, would you kindly respond?

Ms. SANCHEZ-ADAMS. Yes. I agree.

The CFPB, in January 2025, entered a consent order against Block, which is the owner of Cash App, for fraud that was happening there. They were not investigating properly unauthorized-use claims under EFTA. That was one of the violations, as well as a lot of other promises about a system that was safe and was supposed to protect them.

Now, under that order, they are supposed to receive—consumers and victims who were impacted by unauthorized use, that should have already gotten their money back, are supposed to get \$120 million in redress. However, they have not received a penny yet.

I think part of that is, there is a reduced workforce that is not able to do the work that it is supposed to be doing for that reason. So I agree with you that we need to restore the strength of the CFPB.

Mr. GREEN. Yes.

You mentioned Zelle. Explain.

Ms. SANCHEZ-ADAMS. Yes, so they had also—in I believe it was December 2024, they had filed a suit against Zelle for similar infractions. So they also were not responding to the EFTA unauthorized use claims properly, timely, reimbursing impacted victims.

Also, they knew before it was time to launch the product that it was not yet safe and did not have all the guardrails that it may now have in place at the time, because they did not want to lose market share. So the claim in the petition is that they launched it before it was safe, as a violation of the Consumer Financial Protection Act (CFPA).

Unfortunately, as I mentioned in my testimony, with the change of leadership at the Bureau, that suit was dismissed, though it was picked up by the New York Attorney General's Office.

Mr. GREEN. Are you familiar with the Townstone Financial case?

Ms. SANCHEZ-ADAMS. Yes.

Mr. GREEN. Okay. This is invidious discrimination against Black people. Settlement was at hand. Tell us what happened, please.

Ms. SANCHEZ-ADAMS. Yes, in that case, there was actually a court order, and they were ordered to pay back money. The Bureau decided it did not want to pay that money out or to enforce that order and they wanted to vacate that order, and the court did not allow them to do so.

Mr. GREEN. What signal are we sending to consumers when we complain about the atrocities that they have to suffer and we eliminate the agency that is there to help them? What is the signal that we are sending, please?

Ms. SANCHEZ-ADAMS. That we do not care about them.

Mr. GREEN. If we cared about consumers, would we eviscerate the Consumer Financial Protection Bureau?

Ms. SANCHEZ-ADAMS. Not in my opinion.

Mr. GREEN. What could we do to strengthen it, in your opinion?

Ms. SANCHEZ-ADAMS. We do need to restore the funding so that it is able to function the way that Congress designed it to function under the Dodd-Frank Act. We also should not eliminate the workforce that is there to do the job of protecting American consumers.

Mr. GREEN. This is another example of how the President creates a problem and then decides that he will solve the problem with the solution that was already there. This is unbelievable that we would

find ourselves now eviscerating the Consumer Financial Protection Bureau and saying that consumers need protection.

I yield back.

Chairman MEUSER. The gentleman yields.

The gentleman from Georgia, Mr. Loudermilk, is now recognized for 5 minutes.

Mr. LOUDERMILK. Well, thank you, Mr. Chairman.

Before I get on with my main line of questioning—Ms. Benda? No? Oh, Mr. Benda. I am sorry. Yes. My apologies. Ms. Sanchez-Adams suggested simply shifting losses from one party to another. What would this do in practice?

Mr. BENDA. I think we can see an example of that in the U.K. They have a reimbursement framework that she mentioned. If a consumer is fraudulently induced of transferring a payment, they are liable to reimburse, up to 85,000 pounds.

So the hope was that this was going to greatly reduce the amount of scams and fraud out there, spur investment. What unfortunately has happened is that—banks had already heavily invested in anti-fraud and anti-scam protections; scam losses only went down by 1½ percent.

The challenge that it would create for banks, though, here in the U.S. is, not only would it not necessarily reduce scam losses, but it would also put banks in the uncomfortable position of trying to tell American consumers how they can and cannot spend their money.

We talk about sending—we do not want people to send money to someone they do not know and trust. By the time they are ready to make that payment, they believe they know and trust who they are talking to. We have countless stories where you can talk to a family member that could not convince someone not to send money and now you are going to have a bank teller that is going to be responsible for making that decision?

We do not believe that Americans want banks telling them who they can and cannot send money to.

Mr. LOUDERMILK. Okay.

While I have you, Mr. Benda—I apologize—the Georgia Bankers Association brought something to our attention earlier this year. As the chairman of the full committee, Chairman Hill, brought up, we also in Georgia have had a big issue with check washing, especially through the post office—stealing of checks. I mean, hundreds of thousands of dollars have been fraudulently stolen that way.

They brought up a scenario where the fraudster or the criminal would go to a nonlocal bank and, most likely using fraudulent identification, would open a bank account, and that would pass the know-your-customer standards. Then they would take these fraudulent checks and deposit those in that bank but instead of the Big Bank putting a hold on the check, they are paying those checks and clearing them.

Is that a problem that you have been aware of? Is this something that would be an easy fix of requiring the banks to hold the checks?

Mr. BENDA. So check fraud is a very substantial problem that does not appear to be going away.

We have a lot of challenges right now with fake IDs that are out there. If anyone has a college-age student, they know that it is relatively easy. AI is now allowing criminals to generate very realistic-looking statements from a utility company, from a telephone company.

So banks are really struggling with, when the documents being used to open an account look completely legitimate and in many cases pass through certain verification procedures, they will open up those accounts. So what we train banks to do is look at the age of the account, look at the holistic nature of what is being done, what is the pattern of deposits.

So banks would like more flexibility, quite frankly, on being able to hold those checks. Certain checks have certain timelines and when they have to release the funds, such as a Treasury check. So we would be very open to having a discussion of how we could increase those hold times appropriately when fraud is suspected and that is something our members would be very interested in.

Mr. LOUDERMILK. Okay. Thank you for that.

In your testimony, you mentioned that criminals effectively took advantage of the economic devastation during Coronavirus disease 2019 (COVID-19), especially the unprecedented government response to support small business and out-of-work Americans.

How has the COVID-19 pandemic had a lasting effect on fraud?

Mr. BENDA. Well, and I think Mr. Bednowitz mentioned that the identity theft that is out there.

Let me give you the example. We talked about that trust issue that the scammers built. If you get a phone call that comes in, it shows the number on the caller ID of your bank, and they say, "Mr. Loudermilk, is this you? Do you live at this address? Is this the last four of your Social Security number? Can I talk to you about some potential suspicious transactions on your account?"

The vast majority of Americans do not realize that all that information is out there, do not realize their phone number can be spoofed—that the bank phone number can be spoofed, and they are going to believe they are talking to their bank, and they are going to give up that information.

That is the challenge that we face. We face a very sophisticated criminal adversary that is leveraging the loss of all that information and the technology available to them to steal from American consumers.

Mr. LOUDERMILK. Has the pandemic actually helped create new criminal networks?

Mr. BENDA. I believe so. What we have seen is, the unemployment insurance fraud created that market for the personally identifiable information, but it also created a belief that this white-collar crime does not get enforced. So check fraud vastly increased after 2020; identity theft increased after 2020.

These white-collar financial crimes have vastly gone up. Unfortunately, enforcement, due to lack of resources, simply has not kept up.

Mr. LOUDERMILK. Okay.

I see my time has expired, and I yield back.

Chairman MEUSER. The gentleman yields back.

The gentlewoman from California, Ms. Waters, who is also the ranking member of the full committee, is now recognized for 5 minutes.

Ms. WATERS. Thank you very much.

Let me just start by saying, Donald Trump is the most profound—pro-fraud President in history. He dismantled the CFPB, rolled back protections, and dropped lawsuits against Big Banks and crypto scammers, making it easier to basically scam retirees, students, and working Americans.

He is \$7.7 billion richer and continues profiting off the Presidency at the expense of constituents. Under his watch, fraud targeting American consumers has soared, from meme-coin pump-and-dump schemes to insider trading linked to his own tariff announcements.

Ms. Sanchez-Adams, earlier this year, Trump's CFPB, since he took it over, dropped a lawsuit that the agency previously filed against Zelle, Bank of America, JPMorganChase, and Wells Fargo, where they found hundreds of thousands of consumers lost nearly \$1 billion through various payment fraud schemes.

With enforcement cases like this being dropped by the Trump Administration, how will these harmed consumers get their money back?

Ms. SANCHEZ-ADAMS. That is a great question. Thank you for that question.

Unfortunately, right now, they are relying on their State regulators to pursue that enforcement. As I mentioned earlier, the New York AG filed suit against Zelle for the same actions, but that is only protecting New Yorkers, and the rest of the country also needs protection. You do not want to hear from your constituents, "Why are not you doing anything? New York is doing something, but we are not doing anything."

So that would be one answer, is that we need more protection by the CFPB, more enforcement, instead of dropped suits.

Ms. WATERS. Well, let me just say that this hearing is a sham. Committee Republicans are defunding the very agencies designed to protect consumers and oversee the financial system.

Just 2 months ago, Republicans voted to eliminate half of the CFPB's budget—you heard all that discussion this morning—all while rejecting every attempt by Democrats to rein in Trump's crypto fraud. Instead of protecting consumers, committee Republicans have chosen to enable scams and defend Trump's fraud-first agenda.

What can we expect further from the CFPB that has now been reduced to practically nothing, with all of the layoffs and firings, et cetera, et cetera? What can we expect them to do? How much more harm can they rain on the American people?

Ms. SANCHEZ-ADAMS. Thank you for that question.

Unfortunately, taking steps to deregulate the industries that pose a threat and harm consumers is not the right step to take, and I hope that is not what continues. I hope that they do not bend to the pressures of industry to let them do what they want and continue to harm consumers.

I hope that they do continue to enforce laws, and I hope that they continue to do supervision like they are supposed to do, instead of weakening their efforts to protect consumers.

Ms. WATERS. Would you agree that the way that they have defined this hearing, "Fraud in Focus: Exposing Financial Threats to American Families," is misleading?

Ms. SANCHEZ-ADAMS. I hope that we are taking steps to protect families against fraud and not just paying lip service.

Ms. WATERS. Having a hearing like this, where the opposite side of the aisle is talking about "fraud in focus," again, "exposing financial threats to American families," do you think that, based on some of the comments that I have made about the Consumer Financial Protection Bureau and others—I was one of the ones sitting on the conference committee of Dodd-Frank reform when we actually got some protection from consumers with the CFPB—do you think that I have at all missed, somehow, defining correctly what has happened to the CFPB?

Ms. SANCHEZ-ADAMS. No. I think it is accurate that they are not doing the job that they were ordered by Congress to do; they are not currently protecting consumers against harm.

Ms. WATERS. Is there anything that you think they can say to deny anything that I have said?

Ms. SANCHEZ-ADAMS. No. I just hope that Congress restores their funding and they hire their employees back so that they can get back to doing their job.

Ms. WATERS. Thank you very much.

I yield back.

Chairman MEUSER. The gentlelady yields back.

The gentleman from Tennessee, Mr. Ogles, is now recognized for 5 minutes.

Mr. OGLES. Thank you, Mr. Chairman.

Thank you to the witnesses for being here.

Mr. Benda, the banking industry has reported that fraudulent ads purchased through Google and Meta are being used to impersonate legitimate financial institutions, tricking families into handing over sensitive credentials and wiring away their life savings, otherwise known as "malvertising."

When banks flag these ads, what specific obstacles do you face enforcing Big Tech to remove them quickly and are these platforms effectively profiting while dragging their feet on takedowns?

Mr. BENDA. Thank you for the question.

So I think that what we are seeing is significant levels of profiting from these ads. The best source we have is a Wall Street Journal article that said Meta earns \$160 billion from ads. They estimated 70 percent of those ads were either illicit or poor goods or fraudulent ads.

It can take 8 to 32 strikes to take down an ad and so you can imagine someone reporting something 25 times is not sufficient; it has to be 30.

So, I would say, not all social media companies are the same. Google is an example, I think, of a company that is improving. They have a Priority Flagger program where they partner with financial institutions to report things. During the pilot, they took

down ads with—they took down around 97 percent of the ads that were reported within a very quick timeframe.

We think that type of activity needs to be done across all social media platforms, whether voluntarily or mandated but we also think user-sponsored content, which the Google Priority platform does not account for, needs to have a way to be examined when they are portraying themselves as a financial services company and luring people into scams.

Mr. OGLES. Just to clarify, you said Meta, \$160 billion, roughly 70 percent was fraudulent?

Mr. BENDA. That is what The Wall Street Journal reported, sir.

Mr. OGLES. Goodness.

Ms. Griffin, the GAO has found that responsibility for countering scams is spread across 13 Federal agencies, with no real coordinated strategy.

Given that malvertising on Google and Meta is now a common vector for fraud, should national anti-fraud strategy explicitly include requirements for these platforms to vet and verify financial advertisers before an ad ever goes live?

Ms. GRIFFIN. Thank you for that question.

One of the things that was clear in the conversations we had among the task force members, which included the companies we are talking about today, is that there are very different business incentives and legal and regulatory requirements across these different sectors.

We believe that there is an important step to take that outlines the private-sector expectations or responsibilities that companies have for scam prevention and combine that with Good Samaritan legal safe harbors when firms act in good faith to prevent scams.

Doing so, I think, would go a long way toward creating a better playing field for all of these different sectors at the table.

Mr. OGLES. Mr. Bednowitz, your company specializes in monitoring and protecting consumers against identity theft. From your vantage point, how often do victims first encounter fraud by clicking a fraudulent search and/or social media promotion?

Given the sophistication of AI-generated scams, do you believe that Google and Meta's so-called consumer education efforts are keeping pace with the real threat, or are they leaving Americans to fend for themselves?

Mr. BEDNOWITZ. Yes. Thank you for the question, and it is a very good one.

I am looking at data here. From our own protection, we see that 63 percent of scam-related threats were observed on Facebook, 22 percent on YouTube and criminals are using AI-generated personas and deepfakes to make these scams appear legitimate, like what we are talking about here.

There is also another vector of threat from the social media companies by them encouraging people that it is in their best interest for people to have their information publicly and people do not realize that they hide privacy controls. The more information that is out there, the easier that criminals can take advantage of that and use that with AI to put together sophisticated profiles that allow them to target people in the most personalized ways possible.

Mr. OGLES. Well, I want to caution, you know, when you are a hammer—i.e., the Federal Government—everything looks like a nail. The last thing I want is more government, which is why I supported gutting the CFPB. In fact, in a hearing, I said, “To be or not to be,” and I said the one agency that deserves to die the most painful death is, in fact, the CFPB because of the regulatory restraints they were putting on small banks.

That being said, when you look at this issue, the crisis at hand, especially the seniors but in general the scams and the loss of funds, Mr. Benda, what can we do—and we have 28 seconds—what can we do to fix this?

Mr. BENDA. I think one of the things that is critical is to have a takedown process. We recognize these ads are up there. When someone is being impersonated, say, your local banker, and it is scamming people into crypto schemes that need to be taken down and need to be taken down quickly. At a minimum—

Mr. OGLES. Mr. Bednowitz, you will get the last word.

Mr. BEDNOWITZ. I agree with what Mr. Benda is saying. There needs to be vetting of the advertisers on the platform and then also pressure to make privacy controls more transparent to the consumer.

Mr. OGLES. Thank you, Mr. Chairman.

Thank you to the witnesses. You all have a great day.

Chairman MEUSER. The gentleman yields back.

The gentleman from Louisiana, Mr. Fields, is now recognized for 5 minutes.

Mr. FIELDS. Thank you, Mr. Chairman.

Thank you, Acting Ranking Member.

Let me thank all the guests who are here today as well.

In Louisiana, we have been faced with a different type of fraud. We have had—and it is not just the elderly; it is all ages—where a person or group of people will send a text message. The most recent was a text message reportedly from the DMV saying you have to pay a fine, a ticket that happened whenever ago, or you will lose your driving privileges, and they give them a certain time.

I have the email here. Actually, they sent it by text, but it is from an email and the attorney general, obviously, went to work to try to find out the origin of this bad email but there were just good people, young, old, all races of life, all walks of life, and many of them were responding.

What can we do to figure out where the emails come from? Do we have a system in place to do that? That is for all of you.

Because it is hitting our State hard, and it is just paining to hear constituents call and say, “Should I pay this ticket? I do not remember it, but should I pay it?” and then you say, “It is a scam,” you know?

What can we do?

Ms. SANCHEZ-ADAMS. I am happy to take that question, because I have gotten the same text message over and over again.

So part of it is, as we put in our paper, in our written testimony, we have recommendations that tell communication companies what they should do to prevent those types of text messages from hitting consumers. They should do the same thing that banks do of knowing your customer. They should do the exact same thing.

As I mentioned, they know when they are trafficking fraudulent activity; they just do not have the incentive to stop that, which is why we think the FCC and Congress should act to require higher and stiffer penalties. I know that is outside of this committee.

I think we should not wait for them to act; this committee can also act. Part of that is my recommendation that consumers are also made whole and that they are reimbursed for fraudulently induced payments.

We need to have everybody acting to protect consumers.

Mr. FIELDS. Good.

Ms. GRIFFIN. I would like to add to that. Thank you for the question. Certainly, that particular text message is one we are all familiar with.

We spend a lot of time in our task force really talking about the interface between the private sector and law enforcement and their ability to share information with one another about things like this that would create better information for law enforcement to act and better information across the private sector so that, for example, if someone acting on that text message directed their financial institution to send a payment, the financial institution might have information that helps to disrupt or stop that payment.

There are not clear, easy protocols right now for law enforcement and the private sector to be sharing that data. It is a critical element that we will be talking about more in the forthcoming report. Often, in fact, those things are done manually. We heard tales of stacks and stacks of PDF files, with hundreds of pages of raw data and knowing what we know about the ways that we have technologically to be able to share that data, it is an issue that I think we can make some real progress on to be able to strengthen everyone's ability to act.

Mr. FIELDS. Thank you.

Mr. BEDNOWITZ. Thank you for the question.

I would say, there are two ways that we can address this, and I look at this from the consumer angle.

One is awareness, and I come back to this a lot. If people have vigilance—we have to tell people that they can no longer trust communications coming from SMS, email, or phone. Anything that comes, they need to go and verify that. They need to stop, breathe, verify.

The other thing that I would say is, there are solutions in the private sector that can help, that can scan people's emails, texts, and block their phone calls so that these things—they get warnings or they get blocked before it ever reaches them.

There are interfaces that have AI to be able to battle AI, that they can take these communications, put them in, that are trained on millions and millions of scam emails, to say, hey, is this a scam or not? So they also need that level of protection. In a world where the scammers have AI, we need consumers to have AI to defend them as well.

Mr. FIELDS. I am out of time, but I would love to hear your response.

Thank you, I will yield back the balance.

Chairman MEUSER. The gentleman yields back.

The gentleman from Florida, Mr. Haridopolos, is now recognized for 5 minutes.

Mr. HARIDOPOLOS. Thank you, Mr. Chairman.

I first want to express my gratitude to our sheriff back at home, Sheriff Wayne Ivey. He has been very aggressive in getting out the information. As I think everyone in the room knows, this is all about prevention, because the odds of catching these characters are very, very low. It is great to see law enforcement leaders like my sheriff, Sheriff Ivey, getting out there, using social media for a positive, and making sure that people recognize these scams, as each of you are talking about, so that we do not even have these problems to deal with in the first place, because people are aware and I think they are making smarter decisions.

I actually talked to one of my friends today, talking about a financial issue. He said, "Can you please give me a call? I want to make sure it is you asking me this question." I think that this is a lot of the things that we are going through in this real-life world. So I really applaud the locals getting into that.

Ms. Griffin, I would like to ask you first question. I would like to focus on your work with the National Task Force on Fraud and Scam Prevention, which I understand is a working group with law enforcement.

How do Federal, State, and local groups work together so we do not have these different silos, but they actually work in concert, so we are not wasting resources and getting this broad message across?

Ms. GRIFFIN. Absolutely. Thank you very much for the question. I just have nothing but praise for the dedication and passion of law enforcement agents working on this issue across local, State, and Federal agencies.

We heard multiple instances of local task forces where that, sort of, multiplicity of agencies were working together in a local community both to try to deconflict cases and to try to raise awareness in those communities but I cannot stress enough how often we also heard that this was a side-of-the-desk activity, that this was happening in off-hours through the passion and dedication of those agents and not because anti-scam efforts were a dedicated priority of the agencies in question.

We also heard that there is a greater need for more training of local law enforcement agents on how to work with scam victims, so that when a victim does come forward to local law enforcement, which is rare, they are treating that victim in a way that, A, shows compassion, but, B, is able to elicit the information that we need in order to go after those criminals.

Mr. HARIDOPOLOS. Well, thank you.

I will build on the question. I know—just recently, I spoke about it with my other sheriff down in Indian River County, Sheriff Flowers. Almost daily, he has people coming in saying, "I thought this person was this person versus that person," and tens of thousands of dollars. This is not a small scam. This is a serious number, at least in the communities that we are living in.

So how do those local sheriffs share information, Ms. Griffin, across the jurisdiction so that one can quickly get the scam out there?

I know, whenever I get the oddball text, I will often go to one of my search engines and say, is this number real, is this real?

How do we make sure that, once we see a small activity—maybe others can chime in on this as well—that we quickly get the information, so we stop that scam in its tracks and people are alert enough to say, is this real or not?

Ms. GRIFFIN. Yes. No, it is a great question. There are multiple resources available for consumers, but the fact that there are multiple resources available for consumers then makes it also sort of a noisy environment. Where do consumers turn to is a real question, I think, that we need to solve for.

There are also not always easy ways for law enforcement to know what to do in that scenario. We talked earlier today about how the criminals who are perpetrating these crimes are often representatives of foreign criminal enterprises, and so the jurisdiction of local law enforcement is quite limited in that case. So their ability to then liaise effectively with Federal agents who can take action is something that we need to create more strategic and streamlined pathways for them to do so.

Mr. HARIDOPOLOS. Well, thanks, Ms. Griffin.

I will just close with this, Mr. Chairman. I really applaud my local sheriffs, Sheriff Ivey and Sheriff Flowers. They are really aggressive getting out there in their local community, and I am glad that we are raising this awareness. That is probably the biggest weapon we have.

As you mentioned, Ms. Griffin, so many of these criminal syndicates are not within the borders of the United States, and the likelihood of recovering these dollars is very, very slim, given the realities of these crimes.

I think—I know that some folks have talked about the CFPB getting involved in this issue. This is a front-end issue. This is not a back-end issue. The likelihood of us, kind of, coming through with some government agency to recover these are probably pretty slim but I hope that we can use the coordinated efforts for the future so that, when one scam happens, we can use the power of the internet in positive ways so that people realize, if you see this number, beware.

These are just the challenges of the day. It is frustrating. We have so many great innovations coming with social media, but these are clearly one of the detractions from it.

So, with that, Mr. Chairman, thank you for highlighting this issue. It is a huge issue, unfortunately, in our district and the fact that you are bringing this to people's attention will probably save a lot of folks a lot of money.

Thank you.

Chairman MEUSER. The gentleman's remarks are appreciated. The gentleman yields.

The gentlewoman from Georgia, Ms. Williams, is now recognized for 5 minutes.

Ms. WILLIAMS of Georgia. Thank you, Mr. Chairman.

Thank you to all of our witnesses today for your testimony and being here.

I appreciate my Republican colleagues for focusing on this hearing and exposing financial threats and potential solutions to fight

off fraudsters in this space. Y'all, I do need to point out that we had an independent watchdog that helped to protect consumers and deliver dollars back to constituents, and it was the Consumer Financial Protection Bureau, but my Republican colleagues decided in the billionaire bailout bill to reduce funding for the CFPB, leaving opportunities for fraudsters to flourish.

Since Acting Director Vought's takeover of the CFPB, ongoing cases to hold financial institutions accountable for deceptive practices have been dropped. Many of the rules that were either proposed or implemented by former Director Chopra have been dropped as well, all of which were aimed at helping consumers find relief and the most baffling: It is mid-September, y'all, and we still have no clue when the Acting Director is going to testify in front of the full committee. Perhaps I missed the memo, but what we are focused on today is—or, my focus today is on the consumer. The billionaire bailout budget opened the door for scammers, a poisoned CFPB, and pivoting from the previous administration's rulemakings that put consumers over schemers.

Y'all, the schemers are real. I just heard this week a news report down in Columbus, Georgia, where the local sheriff's office, working with the FBI, was at point-of-sale transactions at Target, Walmart, gas stations, pulling the skimmers from the machines, because people's cards were being cloned and purchases being made all over the country.

Then, of course, we are all too familiar with, like my colleague from Louisiana stated, those text messages, where even my 10-year-old son, Carter, is like, "Mommy, I do not drive a car. What do they mean, they are going to take my driver's license if I do not pay?" This is rampant across the board but because of these reductions at the CFPB and all of the changes, I am going to use this time to remind the American people how this administration is prioritizing scammers and fraudsters and hurting our constituents.

Ms. Carla Sanchez-Adams, last December, the CFPB announced at the time that they were distributing \$1.8 billion—with a "B," billion dollars—to 4.3 million consumers, including \$103 million delivered to Georgia, for consumers that were harmed by a group of predatory credit-repair companies. That is real money. This was the largest-ever distribution from the Bureau's victim relief fund in history, and I applaud the Bureau for acting against these scams, but I think we know that there are still widespread financial scams like this that are still ripping off American consumers.

Ms. Sanchez-Adams, have you heard of this type of financial scheme and is this the type of scam impacting customers that you work with?

Ms. SANCHEZ-ADAMS. Yes. So "credit-repair" organizations, quote/unquote, do charge consumers to help them fix their credit. Often, they actually charge and collect that money before actually doing anything to help address some of the credit issues, or they make false promises that they can do something that they cannot actually do. It is indeed a big problem, and I agree with that.

I also just want to take this moment to respond to something that was said, that, like, fraud and scams is a front-end issue and not a back-end issue. I take issue with that, because fraud encompasses both scams and also unauthorized use. I hear so many cases

where consumers are being impacted by unauthorized use, meaning someone takes over their account, someone initiates a transaction without them knowing about it, and yet their banks are not making them whole, even though under the law they are supposed to not just banks, but P2P apps, which is what the Zelle lawsuit and the Cash App lawsuit were about.

That is supervision. That is the Bureau stepping in and saying, “Hey, you guys are not complying with the law. You are supposed to be protecting consumers.”

So I just wanted to clear that up.

Ms. WILLIAMS of Georgia. Thank you for that.

Building upon that and the conversation around the predatory practices around cleaning up your credit reports, do you think there is an opportunity for Congress to crack down on these scams and better protect consumers who are trying to get their financial lives back on track and just trying to live in this economy?

Ms. SANCHEZ-ADAMS. Yes.

Ms. WILLIAMS of Georgia. Ms. Sanchez, I ask because, as someone who spent years paying off my student loans—they are done, y’all. I owe zero student loans.

My husband, that is another story, Chairman Meuser. We are still working on his, but I spent years paying off my student loans. I understand how important it is to understand debt and building creditworthiness. It is still an important issue, to fight off predatory actors in the credit repair space.

I remember, during my first term in Congress, when we were in the majority, then-Chairwoman Waters would hold hearings and testimony from the CEOs of the largest banks. We have not had that in a while, so I hope that is coming.

I see that I am coming up on time, so, Mr. Chairman, I want to leave this last question on the record to get a written response.

What do you say to consumers who the banking industry has failed and who have relied on the CFPB as the final course of action when all else has failed them?

I would love to get that on the record in writing.

[The information referred to can be found in the appendix on page 190.]

Ms. WILLIAMS of Georgia. Thank you, and I yield back.

Chairman MEUSER. Okay. The gentlelady yields.

The gentleman from North Carolina, Mr. Moore, is now recognized for 5 minutes.

Mr. MOORE. Thank you, Mr. Chairman.

Financial fraud is touching every corner of our society, and no demographic is immune. This is not a Republican issue, a Democratic issue. This is an issue that impacts everyone.

From sophisticated AI-driven scams to check washing, you name it, criminals are stealing billions from seniors, veterans, working families, really anybody. I know of stories where these crimes have drained retirement accounts, wiped out savings, and really, if not put in check in some way, erode our financial system.

Ms. Griffin, what I would just ask you is: From your experience, who would you say, who is most at risk of fraud today: seniors, young people, small business, and then, are you seeing any particular types of scams being targeted at any of these groups?

Ms. GRIFFIN. Yes. No. It is such an important question, because, really interestingly, in the survey data that we have been analyzing, there are no discernable demographic differences among the victims.

Mr. MOORE. Huh.

Ms. GRIFFIN. It is perhaps one of the only social problems we have in America with that characteristic. Young and old, urban and rural, different geographies, different races, different incomes—everyone is at equal risk of being impacted by this issue.

I would say, the only other discernable difference is that older Americans lose more money, and I think that is largely a result of them having had more time in their lives to accumulate more money to steal.

Mr. MOORE. The scope of this problem is really staggering. In 2024 alone, the FTC reported that 2.6 million consumers reported being victims of fraud, with a combined loss of a staggering \$12.5 billion. As our witnesses have testified before, we expect the true monetary impact of fraud to be much higher because of non-reporting, et cetera.

Mr. Benda, community banks and credit unions, I know, are devoting enormous resources in fighting fraud, but the threat is larger than any single industry can possibly tackle on its own. Can you describe the scale of fraud that your members are seeing?

Mr. BENDA. Thank you for the question.

It is really hard to describe because, as you said, we do not have accurate numbers. We have numbers that are all over the place.

The one thing we can look at is the trend lines. So both the FBI claimed a 33-percent increase in fraud from 2023 to 2024, and FTC showed a 25-percent increase from 2023 to 2024. So fraud is going up 25 to 30 percent every year, in terms of what we are seeing.

From our members' perspective, we have spent an inordinate amount of time on check fraud, and we have seen that the suspicious activity reports (SARs) being reported on check fraud have tripled, frankly, in the past 4 or 5 years, and that number is not going down.

Then we continue to see the rise of scams trying to convince consumers to send money out and that is simply going to continue to increase.

Mr. MOORE. Right.

Well, let me ask you this. How have the banking regulators been engaged in helping financial institutions fight scams and fraud? As a secondary, have there been any regulatory or interagency fragmentation that has made it harder to respond?

Mr. BENDA. The regulators have not—I will focus on the scam issue. The regulators have not really focused on the scam issue, because it is—I think it is more focused on the front-end thing, which is a consumer being induced to commit some type of act.

So what we would like to see them focus on is ways that we can better share information. We really want to focus on preventing the fraud from happening in the first place and that requires sharing information that we receive from suspicious activity reports, sharing information from law enforcement, and allowing banks and other financial institutions to share information about bad accounts

being used in real-time so those accounts cannot be used to commit fraud.

Mr. MOORE. With respect to this, I mean, would you say that the scams are just—I mean, this is probably a rhetorical question. They are becoming more sophisticated, though, these scams are.

Mr. BENDA. They are. They are. They are using the data that they have stolen. They are using AI to fabricate documents. They are using AI to deepfake voices. They are using AI to commit fraud at scale. It is no longer a simple thing, to spot a phishing email; it is very challenging.

Mr. MOORE. You mentioned AI. That brings me to Mr. Bednowitz.

I will ask you a question. We know AI is a double-edged sword. Criminals are using it, of course, to create more convincing scams, but my understanding is that companies are also deploying it to detect fraud.

How effectively is AI being used in protecting consumers today, and what gaps still remain?

Mr. BEDNOWITZ. Yes. Thank you for the question.

AI is definitely a double-edged sword, and we utilize it in our tools to scan millions of data points to detect fraud in real-time, to detect deepfakes, prevent scams from ever reaching consumers via their email, phone, or text. We are not alone. The private sector is innovating very heavily with AI to combat these scams and these fraudsters.

The gaps that I keep coming back to are just awareness on the side of consumers to be able to adopt these types of protections and to also be aware to breathe and stop, to know that they need to check, that they should not just respond to any email, phone, or text, that they cannot—they have to be vigilant, they unfortunately cannot trust their communications today.

Mr. MOORE. Right.

I know I am out of time, Mr. Chairman. I just will point out, now criminals can actually use artificial intelligence to mimic a loved one's voice. I mean, someone gets a call, and they think they are actually getting a call from a family member or whatnot, saying that they need this or need that.

It is scary, how it is out there and so I appreciate the effort that the industry is making on this.

With that, Mr. Chairman, I yield back.

Chairman MEUSER. The gentleman yields back.

The gentlewoman from Michigan, Ms. Tlaib, is now recognized for 5 minutes.

Ms. TLAIB. Thank you so much, Chairman.

We are talking about all of this, and all I keep thinking about is how paralyzed the CFPB is right now. I mean, this is where the 911 for consumer fraud is.

I mean, romance fraud is up. I have this huge fraud right now—you have to check this out, Chairman—where they say, “Oh, you did not respond to the jury response”—did you hear about this one?—“to jury duty, and a warrant is out for your arrest.” They get these calls, and I had one constituent lose \$11,000 on that one. They are getting so sophisticated, because, you are right, they even have a website with dot-org, like, so—not dot-gov, but dot-org, like,

so it looks real. It almost looks exactly like—and the number that they call them from is the same county number.

All of that to say, CFPB was doing an incredible job, and it is being paralyzed right now. Why? Because it goes after banks that cover up the scams, let us be honest. Let us be frank here. Everybody keeps thinking about that, but think about it. I do not know why they do not want to, like, help and aid in regard to this.

I mean, to see them in March, CFPB, under the current administration, dropped the case against digital payment app—what was it—Zelle, a joint venture between Wells Fargo, Chase, Bank of America, delivering a de facto pardon to the company for failing to protect its users from fraud. We are almost giving them, like, “Hey, well, that is not our fault. We cannot—oh well.”

I mean, that does not make any—there should be a sense of responsibility on the consumer to be protected if these Big Banks are, again, having their consumers, use their service. It does not make any sense to me.

One of the things—and this is to all the witnesses. If banks fail to fulfill their obligations under the Electronic Funds Transfer Act—some protections in there requiring them to investigate customer complaints of fraud. If those banks willfully ignore hundreds of millions of dollars in consumer losses, would you agree that at that moment, they are not going to be held accountable and they are not going to even actually proceed unless we force them to?

I feel like people think they are just going to do the right thing and I am like, “No. CFPB made them do it.”

What I continue to see—I do not care if it is the loan services for the student loans; I do not care if it was the folks targeting the veterans—and some of this stuff never gets headlines. It never gets in the headlines.

I would love to hear from all of you. I mean, you saw this case get dropped and be honest, I think my time—be honest. Do you think them dropping that case exposed a lot of our consumers right now?

Ms. SANCHEZ-ADAMS. So I will jump in really quick.

Ms. TLAIB. Yes.

Ms. SANCHEZ-ADAMS. So the EFTA—one of the brilliant things about that statute is that it actually has a private enforcement—

Ms. TLAIB. She is talking about, for my residents, Electronic Funds Transfer Act.

Ms. SANCHEZ-ADAMS. Sorry.

Ms. TLAIB. I just want them to know. When they see that, they do not know that there are protections in there.

Ms. SANCHEZ-ADAMS. Right.

Ms. TLAIB. They just think it is something to do with transfer of money.

Ms. SANCHEZ-ADAMS. So it does have private enforcement with really strong remedies if it is violated, including punitive damages and treble damages.

However, not everybody can afford a lawyer.

Ms. TLAIB. That is right.

Ms. SANCHEZ-ADAMS. One of the brilliant things about the CFPB is it acted on behalf of all of those who cannot afford—

Ms. TLAIB. I have said that to people.

Ms. SANCHEZ-ADAMS.—a lawyer.

Ms. TLAIB. “Oh, the elder law clinic cannot take the case”—I am serious, Chairman. “They did not take the case; they cannot do any”—I send them to CFPB and sometimes CFPB just calls or sends the letter, an inquiry; gets it fixed like that.

Ms. SANCHEZ-ADAMS. Yes. I——

Ms. TLAIB. I have seen it happen.

Ms. SANCHEZ-ADAMS. I also just want to respond to something that one of the witnesses talked about, which is about private entities that are able to help protect consumers.

Ms. TLAIB. Yes.

Ms. SANCHEZ-ADAMS. Now, that is all well and good, and I love that but there are low-income consumers who cannot afford those services.

Ms. TLAIB. Right.

Ms. SANCHEZ-ADAMS. That is the importance of government agencies——

Ms. TLAIB. I mean, what do you all think, other than, I mean, Ms. Carla here, what do you all think about them dropping the case? You think that was a great idea?

We are talking about \$870 million in losses to the public. This is 1 of 22 enforcement actions, by the way.

Do not be afraid. Was this a good action on behalf of CFPB, to drop that case?

Paul?

Mr. BENDA. I am sorry, Congresswoman. I am not familiar with the case. I cannot speak to that.

Ms. TLAIB. Okay.

How about you, Ian?

So it is okay; they are just not going to enforce the Electronic Funds Transfer Act.

Go ahead, Ian.

Mr. BEDNOWITZ. No, I appreciate the question. I am also——

Ms. TLAIB. Okay.

Mr. BEDNOWITZ [continuing]. unfamiliar with——

Ms. TLAIB. All right.

Mr. BEDNOWITZ [continuing]. the case.

Ms. TLAIB. Kate, you are familiar. You know that CFPB just dropped an \$870 million case against these folks. I mean, Zelle is participating with these banks, and they are letting it happen and pretty much, they are like, “Sorry. You lost that money. We cannot do anything about it.”

Ms. GRIFFIN. Thank you for the question.

One of the things that we talked about a lot in the task force that we have been organizing is the ability, in this example of the text messages, for the banks to get information from the telecommunications companies about that interaction——

Ms. TLAIB. That is right.

Ms. GRIFFIN [continuing]. so that they know whether that case is fraudulent.

Ms. TLAIB. Why do they not just want to——

Ms. GRIFFIN. There are a lot of actions——

Ms. TLAIB. I do not understand why they do not want to help.

Ms. GRIFFIN. Well, I think the issue we will come out with in this report is how we can help all of those institutions to better share information so that they can take more preventative action.

Ms. TLAIB. Yes. Thank you.

I yield.

Chairman MEUSER. The gentlelady yields.

The gentleman from Oklahoma, Mr. Lucas, is now recognized for 5 minutes.

Mr. LUCAS. Thank you, Mr. Chairman.

Thank you to our witnesses for being here today.

Of course, it goes almost without saying, this hearing could not be more relevant to our world today. One of the most pressing topics I hear from credit providers in my district is the growing prevalence of fraud and financial threats to our families and institutions.

According to CFTC, in my home State of Oklahoma, over \$75 million was lost last year in fraud attacks but we know these crimes are severely under-reported and the actual number is most likely dramatically higher.

So let us focus, again, on the core stuff here. All of our Federal agencies must prioritize the effective prevention tools and work together to find and punish bad actors.

So, Mr. Bednowitz, how has your company had success—let us talk about some success here—in fighting bad actors and what are the lessons the Federal agencies could learn from private-sector experiences?

Mr. BEDNOWITZ. Yes, absolutely and thank you—

Mr. LUCAS. You have been in the trenches. Tell us about it.

Mr. BEDNOWITZ. Yes. Thank you for the question.

We protect over 500 million consumers globally from these types of threats, and we do it through a variety of technology solutions that the private sector offers.

I want to say a few things to address the comment earlier. Just because it is private sector does not mean that it has to be something that people cannot afford. There are partnerships, from peers in the industry, between banks and those credit bureaus, that offer free solutions for people to be able to protect themselves. There is the Identity Theft Resource Center that helps people when they have problems, in addition to the paid solutions that are out there but the success is really based on having comprehensive protection of your devices through security, having identity-theft protection. Scam protection is coming out and then there is restoration and remediation and some of these providers, including us, provide support every step of the way when someone falls victim, as well as the insurance to help reimburse them for those losses that they have.

So there are solutions out there.

We have many stories of people—one story comes to mind of an elder gentleman who, as we talk about these bitcoin ATMs, he was tricked into—that money, \$9,000 had come into his account—into giving \$9,000 into one of those ATMs, but because he was covered by our insurance, we were able to reimburse him for that loss.

Mr. LUCAS. Mr. Benda, could you comment on this as well?

Mr. BENDA. Absolutely, Congressman.

So I think what we are seeing is, banks are making some success at trying to combat these scams and fraud, sharing information where they can, but I think the focus really needs to be here on the prevention side of things.

I think we need better sharing from the telecoms in terms of the text messages that are being out there. I think we need better enforcement from the FCC to shut down those telecoms that are sending those bad text messages, but I think there has to just be better information-sharing across the ecosystem. You can share across financial institutions without fear of liability, but social media, telecoms, and others cannot necessarily share that same level of information.

We know that banks file 6,000 SARs a day—suspicious activity reports—a day focused on fraud, but that information never comes back to financial institutions in a manner they can use to prevent that fraud from occurring.

Mr. LUCAS. Continuing with that, Mr. Benda, we have heard a lot about those gaps in the data collection from Federal agencies on the financial fraud.

Can you talk about the need for and expand more on this cross-agency collaboration and whole-of-government approach? I mean, why are the information silos ineffective? You touched on that. Just in a moment, would you—

Mr. BENDA. I did.

Mr. LUCAS [continuing]. expand on that?

Mr. BENDA. Thank you.

I think that is the critical need.

The question you have to ask yourself is—we hear many times, let us say a small bank gets—their local area gets blanketed with these fake fraud alerts. You hear about this. They send these thousands of messages out, and then they overwhelm—one of our small banks got 600 calls a day. We know crimes are being committed at that exact moment. There is no 911. There is nowhere to call to say, how do I stop these text messages, how do I stop this crime from occurring?

We need to have a centralized strategy. Other countries—like, Australia has developed a national anti-scam center, has a national strategy in place. They have seen a reduction in scam losses of 25 percent. We need that type of centralized approach to build capabilities.

Mr. LUCAS. In the few seconds I have left, Ms. Griffin, how can we make sure the Federal Government and its private industry partners stay competitive against bad actors? How do we adapt to emerging threats? This is moving quickly every moment, it sounds like.

Ms. GRIFFIN. Yes. Thank you for the question.

I just want to underscore what Paul is talking about here in terms of the importance and the urgency of a coordinated national strategy that leverages the best of what America has to offer. The innovation, the ability to coordinate are all paramount. We need to create better clarity of expectations of the private sector for their role in helping to prevent scams.

Mr. LUCAS. Thank you very much.

I yield back, Mr. Chairman.

Chairman MEUSER. The gentleman yields back.

The gentleman from Illinois, Mr. Foster, is now recognized for 5 minutes.

Mr. FOSTER. Thank you, Mr. Chairman, and to our witnesses.

I probably stayed up later than I should have last night reading Mr. Benda's excellent testimony. The thing that struck me over and over, reading that, is that identity fraud was at the core of every single one of the frauds, the long list of frauds, whether it is the text message that starts a long romance scam or whatever it is.

The point to stop this is at the beginning, and the tool at hand is to provide people with a means of proving they are who they say they are in an online environment.

Because of inaction by the Federal Government, States are doing this. They are standing up for what is called the Mobile ID, the digital driver's license. This is simply connecting your Real ID-compliant driver's license issued by the State, which is a pretty unique identity that cannot be—it is very difficult to get many fraudulent copies of the Real ID. We have done a pretty good job, federally, on that but then what you do is, you associate that with your cell phone, take advantage of the fact that a modern cell phone is like a security dongle; it has a unique, secret ID in there. It is a unique device in the world and when it gets associated with a Real ID, that allows you to prove you are who you say you are in a legally traceable method online.

Certainly, every time you open a bank account, that has to be an option to people. Because if you talk about the check washing fraud that we are talking about, they say, Okay, you transfer that to a fraudulently opened bank account. Well, guess what. If you are in other countries—just pick your country—say, Korea, if you want to open a bank account, you get out your cell phone and you prove you are who you say you are, and you can open the account like that, because that has been compared against a list of bad actors. You are a single legally traceable person with responsibility for that account.

It does not happen in countries that have done this and the U.S. is falling behind on this. Countries around the world understand that you need to be able to prove you are who you say you are.

We can do everything that we want with trying to identify patterns of fraud and all of the deepfake impersonations, but the bad guys are getting sophisticated too fast for that. The other side of the coin that they will never be able to beat is when you have a cryptographic assurance of being able to prove you are who you say you are.

The tool at hand is the Mobile ID that is being rolled out by many—digital driver's license—rolled out by many States and this is the real answer to this.

I think that we have to use this for Federal Government purposes. We have gotten very close, for Federal Government purposes, to having motion in both the House and the Senate, never in the same session but the time has passed for that.

I think that if industry had access to a simple, efficient way for people to prove they are who they say they are, there would be a huge adoption immediately and a dramatic drop in fraud.

So does anyone—that whole little spiel I just gave, are there any details you think need to be corrected on that? Or do you all agree that is a——

Mr. BENDA. Congressman, if I could jump in there, I would like to thank you for your leadership in this mobile identity space. You have done a great job of pushing that issue forward, so I want to personally thank you for that.

We partner with the Better Identity Coalition. We recognize the value of mobile digital driver's license. We partnered with them to send a letter to the FDIC asking them to make sure that their examiners are aware that we can use those.

We think it is a critical need, to have a reservoir of truth, to be able to go back to those DMVs. Not every State participates in the DMV validation piece. Having mobile driver's license, digital authentication, we think it is critical. We are happy to partner with you going forward on that effort to do anything we can to spur adoption of that.

Mr. FOSTER. Yes. It will be just a tremendous simplification.

One of the big things we were struggling with during COVID, it was costing, like, \$400 to onboard an unbanked person for a bank and that was a huge barrier to getting COVID relief to people that needed it the most.

It did not happen in countries where you say, "Okay, you want your COVID relief check? Get out your cell phone, smile at it, do your biometric login, have that cell phone prove you are who you say you are and authenticate to a bank account," and, boom, there is your COVID relief check.

It is just—it was heartbreaking to see the delays there and the amount of fraud. Hundreds of billions of dollars of taxpayer money stolen by fraudsters because we do not have a decent way to prove you are who you say you are.

Anyway. So I sense there is some motion, some bipartisan motion, to get this to happen, because the level of fraud is just out of control.

Ms. SANCHEZ-ADAMS. I just want to say, until legislation like that is passed, that is why we need to enforce Bank Secrecy Act regulations and do supervision to ensure that fraudulent accounts are not being opened and money is not being laundered that way.

Mr. FOSTER. Yes.

I echo everything that was said by my colleagues about the tragedy of what has been done to the CFPB and the anti-fraud mission of the CFPB is a small part of what—the damage that was done there.

So I just want to thank you all and look forward to actually building some momentum on this.

I yield back.

Mr. STEIL [presiding]. The gentleman yields back.

I now recognize myself for 5 minutes to ask questions.

I appreciate you all being here on a really important topic. I cannot tell you how many constituents I talk to that have been victims of financial scams, problems—in particular, pig butchering, where people are integrating romantic relationships online—purported romantic relationships online and then delving into a financial side.

Later today, I am holding a hearing in particular as it relates to artificial intelligence and AI. There are a lot of positive things that can be done by AI. There are also a lot of challenges.

I just want to touch on how some of the challenges affect this area, about financial challenges.

Mr. Benda, if I can ask you, in particular, how bad actors are utilizing AI in this way and then I want to get into questions, following that, about the ways that we can utilize technology or AI itself to prevent those.

Mr. BENDA. Sure. Sure. There have been a couple things here today, and I will just reiterate some of those.

I think it is the ability to create very realistic and legitimate-looking phishing emails, phishing texts. We are worried about agentic AI that is going to be able to act on its own, can access personally identifiable information, can deepfake voices to make it sound like someone else, and then interact with either banks or other companies who are trying to fraud them.

I think that the scams part of things is really the tragic piece, in that we are now seeing romance scams being committed, because they can change their visage, they can change their voice. It can be someone from overseas of a completely different race, and pretend to be someone else, and interact and try and build that romance scam, build that trust over time, so that someone loses their life savings.

Mr. STEIL. How are financial services firms navigating these new, choppy waters?

Mr. BENDA. Well, I think there are a lot of challenges that we have in terms of the phishing. We have one thing in place; there is a thing called dot-bank where you can actually register your bank's internet domain. It is less resistant to phishing, simply because no one else—you have to be a financial services company to put your website on there.

We have activities, anti-phishing advertising campaigns, such as our "Banks Never Ask That" that is out there trying to inform consumers. So I think a lot of it is really on consumer education to try to make people aware of the problem.

Mr. STEIL. So the consumer education, what the companies are doing. Should our regulators be reviewing whether or not companies are utilizing some of these anti-fraud projection tools?

Mr. BENDA. We would love to partner with the regulators on a consumer education campaign.

Mr. STEIL. Let me build on some of the AI with you, Mr. Bednowitz, if I can. Mr. Benda just referenced AI being used to duplicate voice, to duplicate images. I think that is one of the things that is uniquely challenging.

You can think of fraud against calling maybe a grandma or a grandpa, imitating the voice of a grandson or granddaughter saying that they need assistance, taking that grandparent fraud to the next step. It is uniquely challenging, especially if that sure sounds like your grandson or granddaughter who needs quick help, and, of course, it is a criminal on the other end saying, send \$100 to this location.

How should we be thinking about that or navigating against that?

Mr. BEDNOWITZ. Sure. There are two ways.

There is a low-tech way, which is teaching people to be vigilant and just using safe words. So, across families, if you have a safe word, which is a unique, nonsensical word that no one is writing down, then if someone is actually having a threat, then they can use that safe word, and you know that is actually that person on the other end or not.

Now, on the more high-tech solutions, my company, others in the private sector are building using AI, like you talked about, to help defend against that type of AI, to detect deepfakes, to detect scams and fraud, whether it is coming through video, through voice, through email. So that is absolutely a front in a battle that we are tackling.

AI is also, though, in the background—what Mr. Benda did not talk about—it is less flashy, but AI allows criminals to take information that is out there in the dark web, that is out there in social media sites, data brokers, and create profiles of you to either steal your identity or to target you with very personalized scams.

Mr. STEIL. And to do it with incredible volume—

Mr. BEDNOWITZ. Yes.

Mr. STEIL [continuing]. in a way that was not possible previously.

I will come to you to close this out, Ms. Griffin. How do you think we should be navigating the downside risk of the AI?

Ms. GRIFFIN. Thank you very much for the question.

One of the first things that comes to mind to me is to make sure that our law enforcement is able to use the same tools. When we think about the kinds of data that are available, both in terms of what the private sector has due to consumers reporting to them as well as the kind of data Paul mentioned, the SARs data base, the ability for our law enforcement to deploy AI, as well, to query those data bases and construct cases and go after criminals at scale is a critical element.

Mr. STEIL. I think what you are saying, to bring us home, is, there is downside risk of AI for sure, but there is also massive upside potential to address these frauds and making sure that we do not throw the baby out with the bathwater is going to be incredibly essential as we dive into AI.

We will be having a hearing looking at that later today.

I appreciate you being here.

I yield back and now recognize the gentleman from Ohio, Mr. Davidson, who is the chair of the Subcommittee on National Security, who is now recognized for 5 minutes.

Mr. DAVIDSON. Thank you, Chairman. I appreciate this and really appreciate the work of the committee staff, Chairman Meuser, and others to get focused on fraud.

As chairman for National Security and Illicit Finance, we opened the year up talking about scam centers and consumer fraud. We had a great panel of witnesses, and I think, once again, we have a great panel of witnesses, albeit different witnesses.

So thank you for your work to protect people from these kinds of scams.

It is clear that financial fraud remains one of the most pressing threats to economic security for American families, and there is certainly a lot to cover.

Today, I want to focus my time on elder fraud. These are some of the most evil, contrived schemes that take advantage of our seniors. They have accumulated money; they are just trying to live out their years. These wicked elder schemes have turned into a global enterprise at this point. It is not like a local crime, generally.

So the good news is, fighting elder fraud is an issue that does unite Democrats and Republicans, should unite all Americans. It is time to cut the party-line pushback and make laws to protect our seniors more effectively.

One example here is the Guarding Unprotected Aging Retirees from Deception (GUARD) Act. It is a bipartisan legislation put forth by my colleagues Congressmen Nunn, Gottheimer, and Fitzgerald. While the FBI, FTC, and the Financial Crimes Enforcement Network (FinCEN) are tracking the elder-abuse fraud schemes, the missing piece here is amping up coordination between Federal, State, and local law enforcement. A lot of times when I talk to my prosecutors, they can detect the fraud, but they have a hard time getting the resources. We are working with FinCEN to try to get more of this.

So, Mr. Benda, scams targeting seniors are on the rise. According to the FBI, from 2023 to 2024, there was a 46-percent increase in complaints and a 43-percent increase in revenue losses. How have scams targeting seniors evolved over the years?

Mr. BENDA. Thank you for the question, Congressman.

So I think they have evolved fairly significantly in terms of, we talked about the use of AI in targeting the elderly folks. One of the things that was really interesting was the use of bitcoin ATMs to cash out on these scams.

We mentioned earlier, DC originally has just brought suit against Athena, which is a bitcoin operator that operated for 5 months here in the District. It turns out that—they analyzed the transactions of the bitcoin ATM—93 percent of the transactions of the ATM were fraudulent, 93 percent. The average age of the victim? 71. The average loss? \$8,000. So the question is, is a 71-year-old really going to buy bitcoin at an ATM inside a convenience store? They are not.

So really the challenge is, they are targeting these elderly folks, and they are trying to convince them, whether threaten or cajole them, and they are cashing out through these bitcoin ATMs.

Mr. DAVIDSON. Yes. Thank you for that.

I think, a couple things there that you highlight. The techniques are used—bitcoin ATMs did not exist a long time ago. AI was not around but the other things is these data centers that are making all this possible are on the back end.

So, as a member of the Foreign Affairs Committee, we are seeing, even nation-state-level structuring of data centers to be able to create income for poor countries. They make some of their—a significant portion of their GDP off of helping scam seniors. So this is becoming way beyond the scope of what State and local law enforcement can do.

You highlight one of the ways that they can do it, and certainly bitcoin ATM has been used for fraudulent activity, but I would also highlight that blockchain tracing tools have made it so it is easier to follow the money, in some cases.

So let me turn to Mr. Bednowitz.

How might consumer education, specifically efforts geared toward seniors, help decrease barriers in reporting?

Mr. BEDNOWITZ. Yes. This is a great question and thank you for that question.

Our data shows that, despite elderly consumers reporting in total \$5 billion of fraud, a staggering amount, 67 percent of them think that they are invulnerable, that they are safe from scams and frauds. So there is a huge gap in expectations and reality.

So it is very important to partner with organizations to raise that level of awareness. We have a partnership with the AARP to help any way that we can reach out to these seniors and let them know that they are vulnerable.

Because seniors think, “Hey, it happens to seniors in general, but it does not happen to me. I am smarter than everyone else” and that is the problem; That overconfidence leads them to be able to fall victim more easily.

Mr. DAVIDSON. Yes, I was particularly impressed with the AARP witness earlier in the year in highlighting the nonprofit center that they are working with in Pittsburgh.

I think the complement to that might be a customer-oriented function for FinCEN that works not only with citizens and consumers but with our State and local law enforcement. We will see if we can do that. I think it is a bipartisan answer. The GUARD Act is a good start, but I appreciate your time today.

Chairman MEUSER [presiding]. The gentleman yields back.

We now will have—excuse me. The gentleman from Iowa, Mr. Nunn, is now recognized for 5 minutes.

Mr. NUNN. Well, thank you very much, Mr. Chair and I want to thank the witnesses for being here.

You have all echoed what all of our seniors, what too many Americans already know: This country and the individuals in it are losing billions of dollars each year to sophisticated scams.

In 2024, there were a reported 2.6 million fraud cases in the United States. It resulted in \$12.5 billion being scammed from individuals, many of those dollars going overseas.

These are not just national statistics. They are real, everyday Americans. They are families, friends, communities, veterans, seniors, not just in my district but across the country.

In Iowa, my home State, last year, the attorney general reported receiving more than 13,000 fraud cases and this is a small farm State by comparison to some. It resulted in the loss of \$42 billion.

My office just worked with a 68-year-old veteran who lost \$100,000 to someone he thought he was helping, only to be scammed out of his military pension.

This is why I am grateful to be working with this committee on a bill that we have introduced called the GUARD Act that provides State and local law enforcement better tools to track fraud, as well as the bill we are leading in a bipartisan way, the Task Force for Recognizing and Averting Payment Scams (TRAPS) Act, to really

stop fraudulent payment schemes targeting seniors at a national level, working both locally and strategically to be able to address these issues.

I am also proud to be co-chairing a new-formed caucus called STOP Scams. This is a bipartisan effort on best practices that we should be sharing, and it is one of the reasons I am so grateful this committee is speaking about our scam attacks today.

Mr. Benda, I would like to begin with you. As you know, banks are on the front line. Too often, fraud occurs there, and coordination with regulators and law enforcement happens after the damage has already been done.

Would not a coordinated task force, like what is created under the TRAPS Act, help to address and disseminate best practices before these events occur?

Mr. BENDA. Thank you for the question, Congressman. Thank you for your leadership and thank you for establishing the STOP Scams Caucus. We think more effort; more focus on this can only help.

So we think the TRAPS Act is a good effort to try and coordinate the activities across the Federal Government. We applaud your efforts in that space, and we hope that you will be able to gather information and come up with a consolidated plan moving forward.

Mr. NUNN. Ms. Griffin, I would also like to ask for your input on this.

Look, the task force has called for a national fraud prevention strategy, specifically with the TRAPS Act. Would this help address a nationwide strategy to oppose the type of scams that we are seeing?

Ms. GRIFFIN. Yes. Thank you for the question and thank you for your leadership with your fellow co-chairs in creating the STOP Scams Caucus.

Your question and the efforts of the caucus really represent what is needed here. We talked about this as a whole-of-society or a whole-of-ecosystem approach. There are a lot of jobs to be done. There are jobs to be done by this committee, by other committees here in this building. The efforts of things like the TRAPS Act that really recognize that and name for leadership within the executive branch of government as well to create a national strategy are critically important at this moment.

Mr. NUNN. I think we all want to go one step further here. It cannot just be the role of the Federal Government, trying to solve this. As you note, this is not just a whole-of-government approach; this needs to be a whole-of-Nation approach and that includes our guys on the front line, whether it is a mainstream bank or whether it is the county sheriff.

One of the things we are trying to do is put more resources in the hands of our frontline defenders. We are leading an effort called the GUARD Act. The GUARD Act looks at empowering local law enforcement to give muscle to the strategy that the TRAPS Act would come up with.

Local law enforcement, as we all know, they are at the front lines. They hear the calls. They talk to the senior citizens. They heard from our veteran and, often, they feel powerless in their abil-

ity to help and by the time the Federal Government shows up, as we noted, it is too little, too late.

The GUARD Act provides local law enforcement with tools to act, while the TRAPS Act would establish a Federal coordinating hub.

Would you say the two bills together create both a top-down and a holistic approach and a strategy that right now is not available to too many?

Ms. GRIFFIN. Yes. Thank you very much for that.

I will say that what we have heard from victims are both stories of times when local law enforcement has been enormously helpful and times when local law enforcement has not known what to do and they have turned away in shame.

So the ability to create more resources so that local law enforcement has training and the incentives to be working with victims and elevating this issue is critically important. Thank you for that leadership.

Ms. SANCHEZ-ADAMS. Representative, if I may?

Mr. NUNN. Yes.

Ms. SANCHEZ-ADAMS. I appreciate the TRAPS Act. The one thing that I ask is that it be expanded to not just cover electronic payments but all types of payments.

Mr. NUNN. That is very good. I appreciate that feedback.

Together, I think we need to be able to come up with a strategy, first of all, to be able to implement and help our folks at the local level.

With that, I yield back my time.

Chairman MEUSER. The gentleman yields. The chair thanks the gentleman for his remarks.

Before we adjourn, I ask unanimous consent to enter two documents into the record: one letter from the Consumer Bankers Association discussing the need for cross-industry collaboration, and the other from the Bank Policy Institute discussing how banks, government, and telecoms need to work together to solve this issue.

Without objection, so ordered.

[The information referred to can be found in the appendix on pages 141-164.]

Chairman MEUSER. I would like to thank our witnesses for their testimony today.

I do want to apologize for the earlier remark made by the ranking member that characterized this hearing as a sham. This is the furthest thing from a sham. We are all here collectively to try to work together to correct the escalating fraud that has occurred over the last 3 to 4 years.

I am sure that the results of our work will be preventing such fraud being caused and forced upon thousands and thousands of innocent Americans. So that is our goal, and I look forward to working with you all on it over the next several months and years or whatever it takes.

Without objection, all members will have 5 legislative days within which to submit additional written questions for the witnesses to the chair.

The questions will be forwarded to the witnesses for their response. I ask our witnesses to please respond no later than October 23, 2025.

[The information referred to can be found in the appendix.]

Chairman MEUSER. This hearing is adjourned.

[Whereupon, at 12:07 p.m., the subcommittee was adjourned.]

APPENDIX

MATERIALS SUBMITTED FOR THE RECORD



Response of Ian Bednowitz,
General Manager, LifeLock
Division of Gen Digital, Inc.

House Financial Services Committee

Subcommittee on Oversight and Investigations

Response to the Question for the Record for the hearing entitled: "Fraud in Focus: Exposing
Financial Threats to American Families"

Submitted October 16th, 2025

For consumers who are facing challenges with fraud and scams and feel they have no recourse today, I would reiterate the following approaches they can take to protect themselves:

Always Be Vigilant

For any messages you receive via email, SMS or by phone, do not respond directly. Contact the individual or institution through known contact information. This is particularly important if it involves a financial institution or transaction of any kind.

Take Precautions

Use a password manager, multifactor authentication, safe words and monitor your bank accounts and credit report regularly

Get Expert Help to Support You in Your Protection.

LifeLock provides solutions to monitor millions of data points and alert customers of any issues, with a team available 24/7 if any issues occur to help you resolve them, backed by our insurance of up to \$3m per individual. We guarantee that we will restore any issue caused by identity theft, or we will provide the consumer with a refund. Our comprehensive package with our Norton products also will monitor consumers' phone, SMS and email and alert them to scams before they ever open the message.

In addition, I would reiterate our recommendations for a full-government approach to protect consumers from the waves of fraud and scams that are hitting them and will only increase. We need government to at all levels to make this a priority:

Prevent Fraud Before It Happens

Launch national public education campaigns that cut across age groups, platforms, and communities. These campaigns should provide plain-language guidance on identifying scams, especially for seniors and younger digital natives. Formalize public-private partnerships with schools, nonprofits, and consumer platforms to deliver digital literacy training, especially focused on AI scams and identity fraud. Modernize breach notification standards so that alerts are timely, understandable, and come up with clear next steps for affected consumers.

Disrupt the Scam Supply Chain

Enact stronger oversight of data brokers and digital intermediaries that traffic in the personal information used to build scam campaigns. These entities should be subject to clear accountability for how data is collected, sold, and secured. Equip federal agencies with targeted enforcement tools, including sanctions against known international scam networks and the ability to take down infrastructure tied to repeat offenders. Increase scrutiny of digital advertising platforms and telecom providers that allow fraudulent content to spread. These companies must do more to detect and disrupt scam campaigns before they reach consumers.

Support Law Enforcement and Empower Victims

Provide funding and training for state and local law enforcement to investigate digital fraud and identity theft. Many scams are international in origin, but the harm is local. Police departments need better tools and coordination to pursue these cases.



September 18, 2025

The Honorable Dan Meuser
House Financial Services Committee
Subcommittee on Oversight and Investigations
350 Cannon House Office Building
Washington, DC 20515

The Honorable Al Green
House Financial Services Committee
Subcommittee on Oversight and Investigations
2347 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Meuser, Ranking Member Green and Members of the House Financial Services Subcommittee on Oversight and Investigations,

CBA¹ thanks you for holding the hearing titled “Fraud in Focus: Exposing Financial Threats to American Families.” Your leadership in raising awareness about the growing epidemic of fraud and scams is both timely and deeply appreciated.

America’s leading Main Street banks have 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. Last summer, CBA 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.”² The document sets out an initial roadmap for cross-industry collaboration among financial institutions, technology companies, law enforcement, and the federal government.

CBA subsequently 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 white paper.³

As noted in both the white paper and the roundtable discussion, no single private industry sector can look across all sectors and gather the data and information required to fully assess the magnitude of the problem, detect and report rising fraud vectors or scam schemes, or track perpetrators. The federal government should use existing tools to aggregate and publish consistent and comprehensive data on an ongoing basis that will not only reflect how Americans fall victim to scams but also the scale of the financial impact it has taken on them.

CBA has consistently⁴ advocated⁵ that the banking, telecommunications, and technology industries -in partnership with federal law enforcement agencies - must work together and be better equipped to

¹ The Consumer Bankers Association is the only national financial trade group focused exclusively on retail banking and personal financial services—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 include the nation’s largest bank holding companies as well as regional and super-community banks that collectively hold two-thirds of the total assets of depository institutions.

² https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4897644

³ [2024-07-21-Fraud-and-Scams-Writeup.pdf](https://openbanker.beehiiv.com/p/scamfighting)

⁴ <https://openbanker.beehiiv.com/p/scamfighting>

⁵ <https://thehill.com/opinion/finance/5273422-government-strategy-fraud-scams/>

develop targeted plans to protect consumers. These entities also need access to relevant data to refine their fraud prevention strategies.

Recognizing the urgent need for cross-sector coordination and building on the momentum of CBA's initial roundtable, CBA joined the Aspen Institute-led 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 nation-wide strategy aimed at helping prevent fraud and scams.⁶

CBA welcomes the opportunity to partner with members of the House Financial Services Committee as they raise awareness about the growing epidemic of fraud and scams and work to develop bipartisan solutions to safeguarding the financial wellbeing of your constituents that address this national crisis.

Thank you again for holding this important hearing.

Sincerely,

A handwritten signature in black ink, appearing to read "L. Johnson", with a stylized flourish at the end.

Lindsey D. Johnson
President and CEO
Consumer Bankers Association

⁶ [Aspen FSP | The National Task Force on Fraud and Scam Prevention](#)



Statement for the Record from the Bank Policy Institute

Before the U.S. House Financial Services Committee, Oversight and Investigations Subcommittee

"Fraud in Focus: Exposing Financial Threats to American Families"

September 18, 2025

The Bank Policy Institute welcomes the opportunity to provide input to the Subcommittee on the hearing "Fraud in Focus: Exposing Financial Threats to American Families." Fraud is a growing threat to consumers as well as the security of the U.S. financial system. Unfortunately, when fraud touches a consumer's bank account, it's often too late. Combating fraud requires preventive actions from social media and communication platforms, where many of these cases originate and spread. It also requires coordination among regulatory agencies; intelligence sharing between telecom, social media and banks; and a cohesive federal government anti-fraud strategy.

State of Play

Fraud and scams are proliferating with alarming speed, and artificial intelligence has significantly increased the scale and efficacy of scams and impersonation schemes. According to the FBI's Internet Crime Complaint Center, Americans reported fraud losses exceeding \$16 billion in 2024, more than double the losses reported just three years earlier. Social media and messaging platforms enable criminals to perpetrate illicit activities by impersonating legitimate businesses or government agencies through automated phishing campaigns, spoofed communications, deepfake audio and video, forged documents and other sophisticated tactics.

- According to the FTC, 36 percent of 2024 fraud reports involving a contact method originated via phone or text, leading to \$1.5 billion in losses, and fraud reports involving social media totaled \$1.9 billion in losses, or 15 percent of all reported losses.
- JPMorgan Chase reported that nearly 50 percent of the fraud complaints it received in the second half of 2024 were linked to social media.
- A recent BPI member survey found that, among Zelle-related fraud in Q4 2024, where a contact method was recorded, 37 percent began with a spoofed call or text, while 52 percent involved social media.

Banks invest in technology and controls to detect, prevent and respond to fraud by helping victims. But telecom and social media companies must bear responsibility for the platforms that enable criminals to target victims and perpetrate criminal activity at scale.

Policy Solutions

BPI recommends a comprehensive set of actions that would enhance security and prioritize prevention, especially from platforms where scams and fraud proliferate.

1. Social media platforms should verify advertisers to stop scams before they originate.

Social media companies should adopt “Know Your Merchant” standards, verifying the identity of merchants or brands posting ads on their platforms before those ads go live. The UK, Australia and Taiwan have successfully implemented such ad verification measures.

Social media platforms currently profit from fraudulent ads because illicit actors pay to post their advertisements on those platforms. This can create an incentive to delay or avoid stronger protections. When fraudulent ads or marketplace listings *are* posted and social media platforms are alerted by banks or consumers to their fraudulent nature, the platforms should work expeditiously to take them down, within a timeline determined by regulators. They should also be required to proactively detect and dismantle scam-recruiting and training sites posted on their platforms.

2. The FCC and FTC should require telecom, social media and messaging app companies to monitor their networks and proactively notify victims.

These industries should be required to authenticate calls and messages to address spam, remove scam ads and impersonated profiles and alert consumers to suspicious activity. Telecommunication companies, in particular, should share known scam numbers and message content and enable consumers to report scam messages as opposed to just flagging spam. These actions will help ensure that prevention starts where scams originate; prevention cannot occur after consumers have already been victimized and lost money. As part of this process, the banking regulators should work directly with the Federal Communications Commission and the Federal Trade Commission to establish consistent, enforceable obligations for the telecom and social media sectors.

3. Banks should be given a safe harbor to intervene when necessary to protect customers.

Banks recognize that consumers value quick access to their money, and regulators can and should strike the appropriate balance between anti-fraud due diligence and timely funds availability.

Banks operating in good faith to protect consumers should have a safe harbor from liability when they place such holds. The bank regulatory framework should also modernize rules on checks and funds availability, such as Regulation CC, to avoid a rigid approach that undermines banks' ability to fight fraud.

4. Regulators should enable and encourage real-time, cross-sector information sharing.

Fraud-related information sharing is too reactive, focusing on the cleanup after a consumer has lost funds rather than enabling the quick identification and disruption of fraudulent content and tactics between sectors. Congress and regulators should encourage proactive, real-time collaboration among telecom, messaging, social media and financial institutions by creating a safe harbor to address uncertainty regarding liability and antitrust concerns. These protections could draw on proven models, such as the Cybersecurity Information Sharing Act, which for over a decade has successfully enabled banks to share real-time threat intelligence with each other and government agencies.

5. The U.S. government should establish a National Anti-Scam Strategy to prioritize prevention strategies and align accountability.

A national strategy would elevate this critical issue to the highest federal level and help the United States develop a more cohesive approach. To unify efforts across the public and private sectors, the U.S. should create a White House office led by an official in charge of fraud and scam prevention. The interconnected nature of scams and fraud across the jurisdictions of multiple agencies – for example, fraud that involves payments, social media and text messaging – necessitates a comprehensive, unified national response.

Conclusion

In closing, the banking industry has made significant strides and raised public awareness to help shield Americans' savings from fraud and scams, but lasting success is a shared responsibility. Fraud and scams originate and spread on social media and telecom platforms. Bad actors must be disrupted before they are able to make contact with consumers. To stop scams at their source, these platforms must take preventive action. The banking, telecom and social media industries need comprehensive and coordinated

direction from the federal government, the ability to coordinate and share critical threat information with industry partners and modernized regulations to expand fraud prevention capabilities.

Accompanying this statement is BPI's letter to the Department of the Treasury, the Office of the Comptroller of the Currency, the Federal Reserve and the FDIC responding to those agencies' Request for Information on Payment Fraud. The letter offers detailed, complementary recommendations for strengthening fraud prevention as it relates to the U.S. payments system.



September 18, 2025

Via Electronic Mail

Department of Treasury, Office of the Comptroller of the Currency
 Board of Governors of the Federal Reserve System
 Federal Deposit Insurance Corporation

Re: *Request for Information on Potential Actions to Address Payments Fraud* (OCC Docket ID OCC–2025–0009, FRS Docket No. OP-1866, FDIC RIN 3064-ZA49)

To Whom It May Concern,

The Bank Policy Institute¹ appreciates the opportunity to respond to the *Request for Information on Potential Actions to Address Payments Fraud* (the RFI).² Fraud risk management is an important priority for all financial services providers and a concern for their customers. The Bank Policy Institute, through its technology policy division BITS, has been working with banks and government stakeholders for nearly three decades to help combat fraud. Examples of BPI-led initiatives include hosting executive forums to discuss fraud trends and threats, sharing effective practices for combatting fraud, partnering with the Financial Services Information Sharing and Analysis Center (FS-ISAC) and National Cyber Forensics and Training Alliance (NCFTA) to enhance fraud intelligence services, and engaging directly with other industries to enhance protections.

The fraud threat landscape has shifted in recent years. According to the FBI's Internet Crime Complaint Center (IC3), Americans reported fraud losses exceeding \$16 billion in 2024, more than double the losses reported just three years earlier.³ Financial institutions and their customers are facing increasingly diverse threats, including check fraud, sophisticated impersonations, authorized payment scams, account takeovers, and synthetic identity fraud.

Banks continue to invest in advanced fraud prevention technologies, including machine learning and artificial intelligence, to detect and disrupt these attacks. Yet the same emerging technologies are being weaponized by criminals to automate phishing campaigns, spoof communications, generate deepfake audio and video, forge documents, and mimic identities to bypass verification. These factors combined with the widespread availability of stolen personal and financial data are further fueling scams, account takeovers, fake account creation, and identity theft.

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 Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System; and Federal Deposit Insurance Corporation, *Request for Information on Potential Actions to Address Payments Fraud Request for Information Related to the Executive Order, "Modernizing Payments To and From America's Bank*, 90 FR 26293 (June 18, 2025).

³ 2024 FBI Internet Crime Complaint Center, *Internet Crime Report, Annual Reports - Internet Crime Complaint Center (IC3)*

This rapidly changing environment demands flexible supervisory and policy frameworks that allow institutions to respond to real world threats as they evolve. Banks need the ability to deploy real-time, risk-based interventions; obtain and share data across industries; and adapt to new fraud typologies without being constrained by outdated regulatory requirements or rigid compliance models. The regulatory framework should be updated to enable financial institutions to proactively protect consumers, focusing on the prevention of fraud schemes.

Executive Summary

Protecting consumers and the integrity of the payments system requires a fundamental shift: fraud cannot be treated as a bank-only problem. Fraud and scams are facilitated across various industries, agencies and platforms outside of banking. Thus, effectively addressing payments fraud requires cross-sector accountability, regulatory alignment, safe information sharing, and stronger operational controls to protect consumers, and preserve the trust and resilience of the U.S. payments system. A national strategy, led at the highest levels of government, must establish accountability across all sectors that enable scams. Telecommunications, technology, and social media companies must be required to implement robust anti-fraud programs with clear obligations and consequences for failure to act. Fintechs, which serve as key consumer-facing providers, must also be held to the same regulatory standards as banks to close dangerous gaps in oversight.

At the same time, outdated regulations limit banks' ability to intervene when fraud or scams are suspected. Modernization is essential to give financial institutions the flexibility to act in good faith to protect consumers without fear of supervisory or legal uncertainty. Agencies should authorize fraud holds on suspicious electronic payments, expand exception holds for potentially fraudulent checks, clarify definitions of "altered", "forged" and "washed" checks, and better align Treasury check processing timelines with fraud realities. Supervisory practices must also shift from process-based compliance to outcome-based oversight that supports proactive prevention and consumer protection.

Equally critical is the ability to share information across sectors in real time. Today, legal uncertainty discourages institutions from exchanging the very fraud data that could stop scams before funds leave the banking system. Congress and the agencies should establish safe harbors and guidance to enable cross-industry fraud information sharing, build standardized fraud and scam taxonomies, and reform SAR reporting to create actionable information exchange. Without these changes, institutions are forced to fight alone against adversaries who collaborate with speed and scale.

Finally, as the operator of critical payment rails, the Federal Reserve should embed fraud prevention capabilities directly into its systems—expanding fraud monitoring, standardizing reporting, and supporting Confirmation of Payee to protect consumers against authorized push payment scams. Treasury should also strengthen check verification processes with real-time tools that allow institutions to validate authenticity before funds are released.

Without decisive action, criminals will continue to exploit system gaps, leaving consumers and financial institutions to absorb the losses.

These recommendations are discussed in further detail below (formatted to follow the 5 sections of the RFI). BPI stands ready to work with the agencies to better address these complex issues and to develop a public-private plan to reduce fraud and scams and better protect consumers.

Understanding the Evolving Fraud Landscape

As the agencies consider actions after reviewing the RFI responses, it is critical to start with a shared understanding of how the fraud and scam landscape has fundamentally changed. Not all fraud is the same, and the strategies required to combat it vary significantly depending on the method, the victim's role in the transaction, and the enabling channels used by criminals. Without recognizing these differences, any policy response risks applying a one-size-fits-all approach that will fail to protect consumers and could even impede prevention efforts.

A clear distinction must be made between unauthorized fraud and authorized payment scams, as each demands different prevention strategies, operational responses, and regulatory considerations. Treating them as a single category would undermine effective policymaking.

- In the case of **unauthorized fraud**, the customer does not initiate the transaction. Controls such as login verification, device identification, AI-driven behavioral anomaly detection, and biometrics can be highly effective. In cases in which a bank suspects unauthorized fraud, banks can verify directly with their customers if they are in fact conducting the activity.
- For **authorized payment scams**, criminals manipulate victims into authorizing transfers to accounts controlled by the criminals through romance scams, impersonation schemes, investment scams, or fake invoices. For the resulting payment, the real customer has initiated the payment, and the bank would not know whether or not the customer made that payment due to a scam. To help protect customers in these scenarios a bank would need to resort to subjective and subtle indicators to ascertain whether their customer was an unwitting victim of a scam. Even when bank staff alert customers they are likely the target of a scam, sometimes customers still insist on sending funds to the scammers. These attacks often unfold over days, weeks, or months with fraudsters building trust with the victim via email, phone, text, or social media.

In scam scenarios, authentication tools alone are ineffective because the customer is knowingly (but unwittingly) initiating the payment. Effective intervention requires detecting behavioral red flags, acting quickly, and persuading customers not to proceed, all while balancing consumer autonomy with the broader public interest in preventing scams. Banks have developed programs aimed at mitigating this challenge, but lasting progress requires flexibility, innovation, and shared accountability across industries whose platforms enable these crimes (social media, messaging, and telecommunications). Focusing only on whether a fraudulent payment occurred, without considering the entire life cycle of the crime – including how it occurred and who enabled it – would not be effective and would risk penalizing the institutions that are diligently working to stop it.

Section I: External Collaboration

Meaningfully addressing fraud and protecting the integrity of the U.S. payments system requires looking beyond the traditional banking sector. The current fraud environment, characterized by organized criminal networks, nation-state actors, insider threats, and cross-sector attacks, demands a coordinated national approach to address fraud at an earlier point in its life cycle.

Collaboration must extend to federal law enforcement, the U.S. Treasury, the Consumer Financial Protection Bureau (“CFPB”),⁴ the FTC, the FCC, Department of Homeland Security (“DHS”), the Postal Inspection Service, and private-sector parties whose services and platforms are used to enable fraud, such as social media, telecommunications, and technology companies. These services and platforms are often

⁴ The CFPB, in particular, has joint rulemaking authority with the Board for certain provisions of Regulation CC (Expedited Funds Availability) related to funds availability schedules, consumer disclosures, and exceptions allowing for extended holds to prevent check fraud.

the entry points for scams, yet they have fewer obligations than banks. Combating fraud and scams should be treated as a national priority, with federal leadership collaborating on comprehensive requirements and expectations across all relevant sectors that can combat malicious actors.

The following three recommendations outline initial steps to help close systemic gaps and strengthen prevention.

1.1: The Agencies should work with the FCC and the FTC to ensure all entities in the life-cycle of a scam or fraud event implement anti-fraud programs.

Telecommunications, social media, and technology firms must play a more direct role in helping to prevent fraud and scams facilitated on their platforms. These industries are now central vectors for fraud and scams, yet they lack the same sort of wholistic prevention and consumer protection measures required of banks. Section 230 of the Communications Decency Act has historically shielded these companies from liability for third-party content, which these entities have often cited as a reason for limited intervention.⁵ While Section 230 does not bar proactive moderation, its broad protections have slowed the implementation of more consistent preventative controls that could prevent the initiation of many scams. By contrast, financial institutions are already subject to extensive requirements and obligations for fraud prevention and consumer protection, such as the Identity Theft Red Flags Rule under Fair Credit Reporting Act (FCRA)⁶ and the Office of the Comptroller of Currency's (OCC) Fraud Risk Management guidance⁷. Ensuring that industries exploited by criminals to facilitate fraud implement proactive prevention and detection measures would close existing gaps and strengthen consumer protection.

Criminals are aggressively exploiting these regulatory gaps. On social media platforms, scammers frequently target victims using fake ads for investments or goods, fraudulent marketplace listings, and even recruitment of new scammers in public groups.⁸ Communications and messaging services are routinely abused by criminals through the use of spoofed calls, text scams or "smishing",⁹ and mass text campaigns

⁵ Section 230 of the Communications Decency Act of 1996 ("CDA 230"), codified at 47 U.S.C. § 230(c)(1), provides that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." Courts have consistently interpreted this provision to grant broad immunity to online platforms from liability arising out of third-party content, including fraudulent or misleading posts, ads, or messages. See *Zeran v. America Online, Inc.*, 129 F.3d 327 (4th Cir. 1997) (holding AOL immune from liability for failing to remove defamatory messages posted by a third party); *Force v. Facebook, Inc.*, 934 F.3d 53 (2d Cir. 2019) (extending immunity to claims alleging that Facebook's platform was used to facilitate terrorist activity).

⁶ 16 CFR 681.2 – Identity Theft Red Flags Rule, established under Section 114 of the Fair and Accurate Credit Transactions Act of 2003

⁷ OCC Bulletin 2019-37, "[Operational Risk: Fraud Risk Management Principles](#)"

⁸ According to a May 2025 Wall Street Journal Report, "Meta Platforms, the parent company of Facebook and Instagram, is increasingly a cornerstone of the internet fraud economy, according to regulators, banks and internal documents reviewed by The Wall Street Journal... British and Australian regulators have found similar levels of fraud originating on Meta's platforms. An internal analysis from 2022 described in company documents likewise found that 70% of newly active advertisers on the platform are promoting scams, illicit goods or "low quality" products... Current and former employees say Meta is reluctant to add impediments for ad-buying clients who drove a 22% increase in its advertising business last year to over \$160 billion. Even after users demonstrate a history of scamming, Meta balks at removing them. One late 2024 document reviewed by the Journal shows that the company will allow advertisers to accrue between eight and 32 automated "strikes" for financial fraud before it bans their accounts." [Meta Battles an 'Epidemic of Scams' as Criminals Flood Instagram and Facebook - WSJ](#)

⁹ Smishing, derived from "SMS" and "phishing," is a type of cybercrime that uses deceptive text messages to manipulate victims into divulging sensitive personal information such as bank account details, credit card numbers and login credentials.

powered by SIM farms.¹⁰ These tactics create systemic vulnerabilities that financial institutions alone cannot fix.

Some platforms have begun experimenting with solutions—scam labeling, voluntary takedowns, or fraud warnings—but these efforts remain fragmented and insufficient. A more durable framework should focus on aligning incentives across sectors so that prevention becomes both an economic and compliance imperative.

Federal bank regulators, including the CFPB, working in partnership with the FCC and the FTC, should develop consistent obligations for telecom, technology, and social media companies to implement anti-fraud programs. These programs must focus on preventing criminals using these platforms to initiate scams or fraud which will reduce the number of fraud or scam payments. These obligations should include meaningful consequences for non-compliance and create incentives for innovation in scam detection, customer alerts, and cross-sector prevention.

For social media companies these measures might include:

- Implementing “Know Your Merchant” identity verification standards and verification of ad ownership and brand authorization before ads are published.
- Removing impersonated profiles, fraudulent ads, and scam marketplace listings promptly after identification.
- Providing consumer alerts when suspicious links or content are detected.
- Reporting confirmed scam activity to a national registry and law enforcement in a timely manner.
- Developing standardized, cross-platform consumer reporting mechanisms.
- Actively disrupting scam training and recruitment sites.
- Standardizing reporting and intelligence-sharing processes with financial institutions to protect shared customers.

In the case of telecommunications and messaging providers (including SMS, RCS, iMessage, and OTT services), measures might include:

- Authenticating all U.S. calls through the FCC mandated STIR/SHAKEN standard.¹¹
- Alerting consumers to unauthenticated calls or messages, especially those originating internationally.
- Deploying robust international anti-scam filters to block spoofing and mass campaigns.
- Enforcing anti-fraud standards consistently across Mobile Virtual Network Operators (MVNOs).
- Sharing confirmed scam numbers and traffic data across carriers.
- Enabling consumers to report scam messages in addition to spam.
- Introducing scam alerts like those offered in Google Messages.
- Adopting stronger Know-Your-Customer controls to prevent criminals from using telecom accounts to disseminate scams.

¹⁰A SIM farm is a sophisticated setup that uses multiple SIM cards to send large volumes of messages quickly, often for fraudulent purposes. These farms exploit telecom networks to send bulk scam texts, phishing messages, or create large numbers of online accounts, significantly increasing the risk of scams and fraud. By automating the process, SIM farms allow scammers to target a vast number of people at a low cost, making it easier to perpetrate scams and compromise personal information.

¹¹ STIR/SHAKEN stands for Secure Telephone Identity Revisited (STIR) and Signature-based Handling of Asserted Information Using tokens (SHAKEN). This suite of protocols aims to reduce the prevalence of fraudulent robocalls and caller ID spoofing, which have become significant issues in telecommunications.

By setting consistent standards across sectors, regulators can ensure that prevention begins where scams originate, not just belatedly when funds are already in motion.

1.2: Establish a White House Led National Strategy to Combat Scams

To be most effective, the agencies should support a coordinated national framework led by the White House. Like the Administration's appointment of an AI and cryptocurrency czar, a federal lead for scam and fraud prevention could unify public and private efforts, align regulatory approaches, and drive proactive data-informed mitigation strategies. This is not only about protecting consumers, but also about safeguarding the resilience and soundness of the U.S. financial system against industrialized criminal activity.

As Fifth Third Bank CEO and BITS Executive Committee Chair Tim Spence noted in a recent op-ed, *"America is behind in the scam fight: Why this bank CEO wants a national strategy"*, the U.S. lacks a central office charged with coordinating efforts across industries and sectors.¹² Unlike the U.K., Singapore, or Australia, the U.S. has yet to establish a single point of leadership to drive accountability across enabling platforms, regulators, and law enforcement.

Recent congressional proposals such as the Scam Safe Act (S.2019)¹³ and the Fraud and Scam Reduction Act (H.R. 4936)¹⁴, underscore the urgent need for action. These bills would enhance coordination, data-sharing, and consumer protections, reflecting important steps forward. Yet, their focus remains within legislative and agency boundaries. A truly empowered White House leader, able to work across sectors and government silos, is necessary to ensure integration, accountability, and consistent prioritization.

A dedicated initiative by the White House could:

- Coordinate interagency fraud strategy and oversight.
- Lead partnerships with telecom, tech, and social media platforms.
- Direct law enforcement prioritization of scams.
- Engage diplomatically to press foreign governments on prosecuting cross-border fraud.
- Coordinate at the state level with relation to law enforcement and education programs.

This type of centralized leadership would help the U.S. transition from today's fragmented, reactive approach toward a proactive and unified national framework. This shift would not only better protect consumers but also strengthen the resilience, safety, and soundness of the broader U.S. financial system.

1.3: Hold Fintechs to the Same Regulatory Standards as Banks

Fintechs are now central to the payments ecosystem, yet many operate under lighter regulatory and supervisory regimes. Those licensed only as state money transmitters or partnering with banks often avoid direct federal oversight, creating regulatory arbitrage and gaps in consumer protection. These gaps leave consumers exposed to fraud and scams, which frequently flow through apps like Cash App, Venmo, or crypto accounts where controls are weaker due to less robust oversight.

BPI has previously called for regulatory parity between banks and fintechs through comment letters that stress fintechs must meet the same standards for fraud prevention, customer verification, cybersecurity, and disclosures as banks.¹⁵ Fintech-bank partnerships should also face rigorous oversight consistent with

¹² Spence, T. (2025, April 1). *The federal government needs to lead the fight against scams and fraud*. *American Banker*.

¹³ *Text - S.2019 - 119th Congress (2025-2026): TRAPS Act | Congress.gov | Library of Congress*

¹⁴ *TRAPS Act (H.R. 4936) - GovTrack.us*

¹⁵ See BPI Comment Letter, October, 30 2024; *Regulators Should Take the Reins on Fintech Oversight - Bank Policy Institute*

federal third-party risk management guidance. Regulation must be based on function and risk—not charter or business model.

Consumers generally assume banks and fintechs provide equivalent protections. When weaker rules apply to one segment, criminals exploit the gap consumers misdirect blame. Equal standards for all providers handling consumer funds are essential to protect consumers and preserve trust in the financial system.

Section II: Consumer, Business, and Industry Education

BPI agrees that education is a critical tool, alongside other prevention measures, to protect consumers and businesses from fraud. Banks already have undertaken extensive efforts aimed not only at raising awareness but also at helping customers recognize fraud and scam attempts in real time. Examples of education efforts deployed by banks include:

- In-app warnings during high-risk transactions, especially when sending funds to new recipients.
- Email, SMS, and social media alerts about trending fraud and scam activity.
- Staff training for call center and branch employees to spot customers under duress or being coached by scammers.
- Targeted campaigns addressing phishing, business email compromise (BEC), impersonation, and romance fraud.
- Partnerships with consumer groups, community organizations, and law enforcement to broaden outreach and prevention.

While these efforts are extensive, the federal government plays a vital role in unifying and amplifying fraud education: the government simply can reach more consumers than any individual bank. Coordinated cross-sector campaigns can ensure consistent messaging, greater reach, and targeted outreach to vulnerable groups. Education must also extend to businesses, nonbanks, and technology platforms that interact with payment systems or customer data.

2.1: The agencies should coordinate with industry and other government agencies to promote consistent and coordinated messaging campaigns

The agencies should explore how they can provide leadership in coordinating consistent education approaches. The agencies should lead in coordinating consistent national fraud education. This includes promoting clear messaging on common scams, launching public-private campaigns modeled on initiatives like “Smokey the Bear,” and ensuring inclusive outreach with tailored content for vulnerable groups through community networks and multilingual platforms. They should also support small business education, particularly for nonbank participants and smaller institutions with limited resources. Together, these actions would create a more cohesive and effective national strategy for fraud education and prevention.

Section III: Bank Regulation and Supervision

The current regulatory and supervisory framework must evolve to meet the realities of today’s rapidly changing fraud and scams landscape. Consumers and financial institutions face unprecedented threats, from large-scale check fraud schemes and account takeovers to scams that manipulate consumers into authorizing payments to criminals. Yet the regulatory tools and oversight environment have not kept pace, hampering efforts to quickly and effectively combat these crimes. Regulation and supervision must shift from rigid process enforcement to a more flexible approach that prioritizes fraud prevention as a core component of both consumer protection and safe and sound banking.

Banks are increasingly placed in a difficult position when balancing fraud prevention with regulatory and funds availability requirements. If they intervene to help prevent a suspected fraudulent transaction, by holding funds or restricting account access – they risk liability under Unfair, Deceptive, & Abusive Acts and Practices (UDAAP) or other regulations. If they do not, they risk being faulted for inadequate controls exposing themselves to fraud losses, or reputational harm. This conflicting environment ultimately undermines consumer protection. The regulatory framework must be modernized to give banks the flexibility to act decisively against evolving fraud threats without fear of punitive consequences for reasonable, risk-based measures.

In relation to the RFI questions on Bank Regulation and Supervision, BPI provides recommendations below focused on two areas: 1) Modernizing regulation and supervisory approaches aimed at protecting customers, and 2) Modernizing Regulation CC to better manage fraud and improve check processing.

Modernizing regulation and supervisory approaches aimed at protecting customers (3.1 - 3.2)

As fraud threats increase and faster payment options expand, financial institutions need updated regulatory flexibility to detect and pause suspicious transactions—both inbound and outbound—in real time. Banks currently have limited ability to temporarily hold suspicious electronic deposits to verify legitimacy, especially in scam scenarios, where manual review or confirmation with the originator may be necessary. Criminals will often move money from accounts as soon as those funds become available, making it critical that banks can hold these payments when a fraudulent transaction or scam is suspected. Given the complex nature of today's fraud and scams, these investigations can take time and banks need flexibility in applying the appropriate holds.

While some institutions have implemented fraud detection tools for incoming electronic payments, there is no clear regulatory authority to pause, review, or return suspicious funds before they are credited to an account and made available for withdrawal. In practice, account-level restrictions have become an essential tool for preventing additional losses once fraud is suspected. For example, when a receiving bank is notified that a payment was sent to a potentially fraudulent account, it must investigate whether the recipient is an innocent customer or a complicit money mule.¹⁶ These investigations are complex, time-intensive, and subject to regulatory uncertainty. Conflicting guidance from examiners and concerns about UDAP/UDAAP liability risk discourage banks from applying holds—even when the intent is to protect consumers. A 2022 CFPB consent order illustrates this challenge, where a bank's fraud-prevention practices led to penalties despite being aimed at blocking fraudulent deposits.¹⁷

3.1: Create a framework for fraud holds for electronic payments and enable banks to effectively manage anti-fraud measures and funds availability.

Other applicable laws, such as the anti-money laundering provisions of the USA Patriot Act, should permit banks to place extended holds on electronic deposits based on suspected fraud without violating the next business day availability requirements of Regulation CC (12 C.F.R. § 229.10(b)). The Board, the CFPB, and the other Federal banking agencies should not construe the Expedited Funds Availability Act ("EFAA") and Regulation CC as operating in a vacuum but should acknowledge that expedited funds availability requirements must work in tandem with laws and regulations focused on fraud prevention, anti-money laundering, and counter-terrorist or other illicit financing. To address this, the agencies should explore the following actions:

¹⁶ A money mule is someone who receives and moves money that came from victims of fraud. Some money mules know they are assisting with criminal activity, but others are unaware that their actions are helping fraudsters.

¹⁷ Consumer Financial Protection Bureau. (2022, December 20). [Consent order: In the matter of Wells Fargo Bank, N.A.](#) (File No. 2022-CFPB-0011). U.S. Government.

Item-Level Holds for Electronic Deposits

- The Board should adopt a new comment to Section 229.10(b) of Regulation CC clarifying that, although the exceptions in Section 229.13 do not apply to electronic payments, other fraud-related and AML obligations may supersede the obligation to provide next-day availability.
- Alternatively, the Board and CFPB could amend the interpretation of when an electronic payment is received under the EFAA and Regulation CC to add a third prong under 12 C.F.R. § 229.10(b)(2) which defines when an electronic payment is received to include “and (iii) complied with the bank’s policies on reasonable fraud screening processes.” This third prong would allow banks to use fraud screening tools to detect potentially fraudulent transactions and investigate such transactions before making the funds available.¹⁸
- Reasonable fraud screening practices could include:
 - Use of prudent processes designed to identify transactions at risk of fraud or scams
 - Use of fraud-imaging or fraud-logic tools predictive of high return rates
 - Detection of anomalous activity through AI, machine learning, or behavioral models
 - Notification from the sending institution confirming suspected fraud or scam
 - Evidence of unauthorized account access
 - Evidence the customer is a suspected scam victim

Account-Level Restrictions

- The agencies and the CFPB should engage with industry to confirm that banks may impose temporary account restrictions to protect consumers, including expectations for communication, documentation, timeframes, and safe release of funds when there is reason to suspect fraud or scam.
- Guidance should leverage the criteria above for a broader “reasonable cause to suspect fraud or scam” standard, enabling banks to act decisively while minimizing disruption.
- Banks should have sufficient time for investigation, particularly in first-party fraud scenarios, before funds are withdrawn or dissipated.
- Institutions should have a safe harbor from regulatory action when holds or restrictions are applied in good faith to protect consumers.

Regulatory Authority to Block or Delay Payments Based on Risk

- Banks must be able to delay or block payments when scam indicators are present, even if the customer appears to authorize the transaction.
- The agencies should work with the CFPB, which has authority under both the EFAA and the Electronic Fund Transfer Act (“EFTA”), to propose regulations regarding disclosure of the terms and conditions of the consumer’s account. Effective disclosure of potential fraud prevention restrictions, and how they may affect the availability of check, cash, and electronic payment deposits, provides transparency and can help reduce consumer complaints. Effective disclosures also help mitigate UDAP/UDAAP risk. For electronic payments (other than wire transfers), the EFTA and Regulation E permit financial institutions to include in their initial disclosures account-level restrictions on the amount and frequency of transfers. These disclosures could be construed to give financial institutions the ability to disclose that they may defer or delay the processing of EFTs for a reasonable period of time to allow for the application of effective fraud detection and fraud prevention measures when they have a reasonable suspicion of fraud or a scam.

¹⁸ The new regulation would read payment is not received until the bank has (i) received “payment in actually and finally collected funds”; (ii) received “information on the account and amount to be credited”; and (iii) complied with the bank’s policies on reasonable fraud screening processes.

- The agencies, along with the CFPB and FTC, also should make clear that a bank has ability to intervene and delay or block payments when scam indicators are detected, even if the customer appears to be authorizing the transaction, and not be vulnerable to violating UDAP or UDAAP or other laws for delaying or blocking payments. The agencies should work with the CFPB and FTC to ensure consistent UDAP/UDAAP guidance regarding permissible payment holds, delays, or blocks.

Additional Regulatory Clarity

- Banks would benefit from having a clearer direction on incorporating age-based fraud risk factors into prevention strategies without violating fair lending laws, particularly the Equal Credit Opportunity Act (ECOA) and Regulation B. Fraudsters disproportionately target elderly populations, and banks need safe, consistent parameters to incorporate this risk factor responsibly.

3.2: Focus Supervision on Effective Fraud Prevention

To effectively combat fraud and scam threats, the supervisory framework must shift from box-checking compliance to collaborative, outcomes-based oversight that prioritizes prevention and consumer protection. Today, exams too often focus on technical procedures or isolated control gaps rather than whether banks' actions are effective in reducing fraud. For instance, examiners may flag account restrictions without acknowledging that such measures were taken to prevent suspected fraud and protect consumers.

This narrow approach risks distorting supervisory objectives. Examinations should evaluate bank actions in context, weighing process issues against fraud-prevention outcomes. Compliance and safety-and-soundness oversight should both support effective prevention programs, aligned with each bank's documented fraud risk tolerance and ability to adapt to emerging threats.

A modernized model would also use exams to surface trends, encourage regulator-bank information sharing, and highlight systemic issues such as cross-platform scams and novel attack methods.

Ultimately, supervisory oversight should enforce accountability while also enabling banks to dedicate more capacity to the shared mission of protecting consumers and the integrity of the payments system.

Modernize Regulation CC to Better Manage Fraud and Improve Check Processing (3.3 - 3.5)

The regulatory framework for check deposits and collections is outdated, fragmented, and ill-equipped to address today's elevated fraud risks and modern payment technologies. Rules are dispersed across Regulation CC, the Uniform Commercial Code (UCC), electronic check image exchange network rules (ECCHO), Treasury regulations, agency guidance, and varying bank agreements. Further complicating this state of affairs is the fact that states have adopted different versions of the UCC, which is further subject to varying interpretation by different courts.¹⁹

Check fraud has surged in recent years, driven by mail-system vulnerabilities, widespread availability of check-washing tools, and criminals' focus on exploiting this antiquated payment method. Between March 2020 and February 2021, the U.S. Postal Inspection Service received over 299,000 mail theft complaints, a 161% year-over-year increase. From February to August 2023, FinCEN logged 15,417 mail-theft-related check fraud reports involving \$688 million in losses. At the same time, stolen check data are openly sold on

¹⁹ Further penalties arising out of such activities may also be grounded in Unfair Deceptive Abusive Acts and Practices (UDAAP) by financial institution regulators.

the dark-web²⁰ and social platforms such as Telegram²¹, enabling organized criminal rings to conduct large-scale forgery, alteration, and counterfeit schemes.

The surge in check fraud has left banks with high volumes of claims and disputes, exposing the limits of outdated legal and operational processes, creating delays for customers and disproportionate burdens for smaller financial institutions lacking the resources to absorb rising losses or manage complex disputes.

Absent a wholesale restructuring of the check collections process (which regulators have acknowledged was based on the presumption that banks generally handle checks in paper form),²² the regulatory framework for check collections and funds availability requires enhancement to provide clarity as to parties' rights and obligations, streamline interbank dispute resolution processes, and facilitate fraud risk management and prevention. Below we provide recommendations for modifications to the existing regulatory framework to help solve these critical challenges, while striking a balance between fraud risk management and expedited funds availability. In addition to the below recommendations, we encourage discussions between the agencies and financial institutions on a roadmap to reduce and eventually eliminate paper check usage.

3.3: Allow banks to place exception holds on check deposits specifically when a fraud or scam is suspected

The current exceptions defined in Regulation CC, including the "reasonable cause to doubt collectability" provision, are not sufficient tools for mitigating check fraud. As currently framed, the Board's guidance for circumstances in which the exception may be invoked primarily pertain to the likelihood that funds are available in the drawer's account. This guidance does not clearly provide that fraud-related anomalies, such as sudden changes in the deposit customer's behavior or high-risk deposit patterns, can be considered when placing a hold under this exception.²³ Furthermore, "reasonableness" standards are largely open to interpretation, further complicating compliance and exposing supervised institutions and consumers to risk.

To effectively combat fraud, banks should have the flexibility to place holds based on the deposit bank's own fraud detection systems, evolving fraud trends, and other risk-based indicators. Fraud prevention controls vary depending on available technology, internal operations, and criminal tactics, and banks must be able to apply deposit holds using a holistic assessment of risk, not just availability of funds or account tenure, which alone are insufficient indicators of fraud.

BPI recommends the Board and CFPB revise the "reasonable cause to doubt collectability" exception to encompass situations where a bank has a good-faith belief that an item is unusual or suspicious and may be the result of fraud. Alternatively, the Agencies could recommend that Congress amend the EFAA (12 U.S.C.

²⁰ Reports suggest that listings on the dark web for "check bundles" range in price from \$1,000 to \$100,000. [Mail Theft, Dark Web Sales, and Counterfeits: Combating Today's Check Fraud Threats](#), SQN BANKING SYSTEMS

²¹ NBC4 Washington. (2023, February 14). [Criminals use Telegram to recruit 'walkers' as America's big banks see an 84% increase in check fraud](#). NBC4 Washington.

²² 76 Fed. Reg. 16862, 16862 ("Subpart C's provisions presume that banks generally handle checks in paper form. Since the provisions were adopted in 1988, however, banks have largely migrated to an electronic interbank check collection and return system.").

²³ The Board's current guidance identifies the following examples of circumstances under which this exception may be invoked, each of which pertain to the likelihood that funds are available in the drawer's account: (i) information received from the paying bank regarding the actual or likely nonpayment on a check (e.g., due to insufficient funds, stop payment order); (ii) stale or post-dated checks; (iii) reasonable belief that the depositor is engaging in kiting activity; and/or (iv) reasonable belief as to the insolvency or pending insolvency of the drawer of the check or the drawee bank. 12 CFR part 229, App. E, § F.229.13(e)-2

§ 4003) to establish a *new exception* allowing for holds on checks in circumstances where fraud or scam is suspected.

As an alternative to the existing reasonableness standard, the revised (or new) exception should make clear, in regulation or commentary, the basis upon which it can be invoked when a bank has a good faith belief of “unusual” or “suspicious” (likely fraudulent) activity based on a customer’s risk profile and indicators such as:

- Use of reasonable and prudent processes and procedures to identify transactions at risk of fraud or scam.
- Reliance on fraud imaging analysis tools or fraud logic rules validated to predict high rates of returns.
- Detection of unusual or anomalous activity through machine learning, AI, or other anomaly-detection models.
- Evidence suggesting a customer is a victim of a scam or other fraud.²⁴

Updating the exception framework in this way would give banks the necessary flexibility to apply risk-based holds in good faith, enabling earlier intervention against fraud while preserving consumer protection and maintaining confidence in the safety and soundness of the payments system.

3.4: Revise the definition and exception for “new accounts” to better align with risk trends

If updated, the “new accounts” exception is another that could be very helpful to institutions as a fraud prevention measure, as many fraud cases arise in the early life of an account. The exception narrowly defines a new account to an account opened in the last 30 days. Fraudsters exploit this by opening accounts, letting them “age,” and conducting small-dollar transactions to build a veneer of legitimacy before committing large-scale fraud.

The rule also fails to provide hold authority for new accounts added to an existing relationship. Criminals are aware of this loophole and often open additional accounts to avoid new account holds altogether. This practice makes it difficult for banks to intervene, even when fraud risk is high.

Expanding the scope of the new account exception, through statutory or regulatory changes, would strengthen banks’ ability to apply risk-based holds to suspicious accounts, verify authenticity of customers, and detect unauthorized or fraudulent activity before losses escalate. Therefore, we recommend consideration of the following actions:

- The Board and the CFPB should close the loophole for customers that hold another account with the depository bank and allow for an account to be treated as a “new account” whenever there is a change in authorized signers or account titling.²⁵
- The time period during which an account is deemed a “new account” should be amended from 30 days to 120 days. This would allow institutions to establish an understanding of account/transaction behavior and afford customers appropriate time to report unauthorized activity, considering standard monthly bank statement cycles.²⁶
- All check deposits should qualify for the “new accounts” exception and eliminate the special rules for greater next-day or second-day funds availability for certain types of check deposits (including

²⁴ These criteria should be used to replace the existing reasonableness standard as it relates to fraud related holds.

²⁵ This could be done by eliminating the language within Regulation CC, 12 C.F.R. § 229.13(a)(2) stating that “An account is not considered a new account if each customer on the account has had, within 30 calendar days before the account is established, another account at the depository bank for at least 30 calendar days”.

²⁶ This change would likely require that Congress amend the EFAA (12 U.S.C. § 4002(a)).

certain Treasury checks, USPS money orders, state or local government checks, and cashier's, certified, or teller's checks) but maintain the requirement for next-day or second-day availability up to the first \$6,725 of funds deposited on any given banking day.²⁷

3.5: Revise Regulation CC's "Presumption of Alteration" provision and Clarify Key Terms

The surge in sophisticated check fraud, combined with widespread use of truncation and image exchange, has exacerbated confusion over how to classify and resolve fraudulent items. Banks face persistent disputes over funds availability, return obligations, fraud type determinations, and liability allocations. A central challenge is the lack of clarity and consistency in defining fraudulent checks. The distinction between "forged maker," "altered," and "counterfeit" checks has grown increasingly blurred as modern methods—such as chemical "check washing" and digital alterations—combine elements of forgery and alteration.

The existing framework under Regulation CC and the UCC, developed in an era of paper processing, fails to address these typologies. Courts have struggled to apply outdated definitions, producing inconsistent rulings that often hinge on technicalities. These gaps prolong interbank disputes, drive up costs, and ultimately delay access to funds for consumers.

Check "washing" illustrates the problem. Some banks and courts treat a completely washed check, which includes washing of the signature, as a forged maker's signature, assigning liability to the paying bank. Others classify it as an alteration, shifting responsibility under presentment and transfer warranties to the bank of first deposit.²⁸ Disputes intensify when the fraudster substitutes a signature with a different name, further complicating the classification.

The Board's 2018 "Presumption of Alteration" was intended to clarify who should hold the loss when only an image of the original paper check is able to be produced as evidence given the split decisions in the courts at the time and to simplify these disputes but has, in practice, created additional ambiguity.²⁹ When the original paper check is no longer able to be produced as evidence in a check dispute, the rule provides an evidentiary presumption that check was altered unless proven otherwise.³⁰ Yet the ability to rebut the presumption depends on producing either the original paper check, i.e., the "original check," which is rarely available in today's environment, as the vast majority of checks are cleared via electronic check image exchange. Only the bank of first deposit has the ability to require its own customers deposit the physical original paper checks rather than use of remote deposit capture. Paying banks can no longer demand presentment of the original paper check before being liable on the item. Other forms of rebuttable evidence can be used, including other images of validly issued checks for comparison of the check stock features which survive truncation. The reliance on a "preponderance of evidence" standard often leads to costly expert testimony, undermining efficiency and encouraging litigation.³¹

²⁷ This change would likely require that Congress amend the EFAA (12 U.S.C. § 4002(a)(1) and 12 U.S.C. § 4003(a)(3)).

²⁸ *Fidelity Brokerage Services LLC v. Pacific Western Bank*, No. 2:23-cv-09760-RGK-MRW, 2024 WL 4874558 (C.D. Cal. Sept. 20, 2024) (distinguishing between checks that were never validly issued and those that were validly issued but subsequently modified to reflect an intention contrary to that of the drawee); see also *Provident Savings Bank, F.S.B. v. Focus Bank*, 548 F. Supp. 3d 862 (E.D. Mo. 2021) (finding that a digitally altered copy of a check which is unauthorized, modified and printed on new check paper is not an alteration under the UCC, and *Provident* clarified that a "washed" or altered check is not a forged maker check, reinforcing the UCC's distinction between alteration liability and forgery liability, which continues to influence check fraud disputes today).

²⁹ 12 CFR § 229.38(i)(1)-(3).

³⁰ 12 CFR § 229.38(i)(1)-(2).

³¹ *Id.*

Given the prevalence of check washing and evolving fraud methods, the Board should reassess whether the presumption is serving its intended purpose. Specifically, it should (i) define “original check” more precisely, (ii) clarify distinctions between altered and forged items, and (iii) issue guidance on satisfying evidentiary standards without reliance on paper checks or expert testimony.

While broader changes to the UCC require lengthy processes across multiple jurisdictions, the Board—working with other agencies—is well positioned to lead a targeted initiative. A working group of banks, trade associations, and other stakeholders should be convened to examine current typologies, develop updated definitions, and establish liability rules that reflect which institution is best placed to prevent losses given modern processing and technology. Harmonizing definitions across Regulation CC and the UCC would promote clarity, streamline dispute resolution, and strengthen the fraud-prevention ecosystem.

While the Uniform Law Commission plays a central role in this context, the UCC rulemaking process is long and cumbersome, requiring adoption by every state, and still open to varying interpretations. BPI recommends that the Board, in coordination with the other agencies, establish a small and targeted working group of banks, trade organizations, and other key stakeholders in an effort to: (i) examine current check fraud typologies and trends; (ii) develop definitions to delineate and clarify different types of fraud and, in particular, define check “washing” in a manner that makes clear whether such fraud constitutes an alteration or a forgery; and (iii) clarify the economically sensible allocation of liability for washed checks, taking into consideration which bank is best able to prevent fraud losses at the lowest cost in light of contemporary check processing methods. While changes in fraud-related definitions ideally should be made in, and harmonized across, Regulation CC and the UCC, BPI believes that the Board is uniquely positioned to spearhead this effort given its expertise in check processing and the regulation of check payments.

A revised definitional and liability framework should incorporate the following principles:

- Provide Clarity and Consistency on Definitions
 - Clarify definitions and distinctions of what constitutes an “alteration” and “forged maker” or “unauthorized signature” considering modern check fraud typologies, including “washed” checks, “cooked”/“baked” checks, and digitally altered signatures.
 - Ensure definitions are universally understood and in alignment with the UCC framework.
 - Clarify what constitutes an “original check” and “alteration” within the Presumption of Alteration considering modern check fraud typologies, including “washed” checks, “cooked”/“baked” checks, and digitally altered signatures.
- Support Efficient and Fair Loss Allocation
 - Maintain the principle that liability rests with the institution best positioned to prevent loss.
 - Balance responsibilities between depository and collecting banks, considering fraud-prevention capabilities, customer protection, and funds availability/return deadlines.
 - Facilitate cooperation between institutions by reducing the adversarial posture created by the current definitional gaps.
- Adapt to Evolving Fraud Methods
 - Incorporate flexibility to address new fraud methods and technologies without requiring wholesale regulatory overhaul.
 - Account for the practical challenges of identifying altered or counterfeit checks.

BPI has spent substantial time working with its members to evaluate definitions and solutions and are happy to participate in this effort.

3.6: Align Treasury Check funds availability timelines for consistency and streamline check return timelines

In response to the Agencies' question on shortening funds availability, we believe accelerating availability would give fraudsters quicker access to funds and reduce the time institutions have to investigate suspicious activity. It would also heighten cross-channel risks, as criminals could exploit the lag in check clearing against the instant, irrevocable settlement of wires, RTP®, or FedNow® transfers. Depository banks depend on fraud-detection tools and need sufficient time to review deposits and apply holds when warranted. Shortening deadlines would weaken these protections and increase fraud losses. Instead, the Agencies should allow banks to extend availability when a high likelihood of fraud exists (as outlined in item 3.3 above) while keeping standard timelines for the vast majority of checks.

Treasury check fraud continues to be a significant challenge for financial institutions, not just due to the rates of fraud, but also misaligned frameworks for funds availability and return obligations banks are subject to versus Treasury. Therefore, depository banks would benefit from additional time to review Treasury checks before making funds available.³²

Treasury has up to 60 days to determine whether a Treasury check bears a forged or unauthorized drawer's signature and to then reverse payment. In contrast, banks only have until midnight of the day following the day of presentment to pay or return a check. Treasury can also process a reclamation for a year and in some cases even longer. We recommend the Board, in collaboration with Treasury and other relevant bodies, explore regulatory solutions to shorten timeframes in which Treasury can automatically reverse payment on Treasury checks, encourage earlier identification of fraudulent government payments, and reduce associated losses for depository institutions. As Treasury moves toward eliminating Treasury check issuances in general, there will continue to be exceptions and by implementing these proposed changes, fraud involving the remaining check volume could be significantly reduced.

Although Treasury provides banks the ability to access Treasury's Treasury Check Validation Service (TCVS), banks typically accept the Treasury check for deposit processing before validating against the standalone TCVS system to determine if the Treasury check is on the list, if it matches as to the dollar amount, check number and payee name and the status of whether the check has already been paid. If it is not valid, the bank then needs to take action to hold the funds pending a return or reclamation claim from the Treasury. A better approach would be for Treasury to implement a positive pay with payee name process so that Treasury checks could be automatically returned upon presentment for payment, affording banks time to reverse any provisional credit to the deposit customer and saving Treasury the time and expense of processing a late return or reclamation.

Section IV: Payments Fraud Data Collection and Information Sharing

BPI appreciates the agencies' recognition that fraud mitigation requires not only strong bank controls but also a robust, data-driven ecosystem for understanding and responding to threats.

Information sharing of actionable fraud indicators in near-real-time is essential to disrupting fraud. There are various types of intelligence sharing that support different, but equally important, outcomes:

³² Next-day availability for these checks is established by the Expedited Funds Availability Act, 15 U.S.C. § 4002(a)(2)(A), and statutory amendments may be necessary to extend the funds availability requirements for these checks.

- **Fraud Data Sharing:** Near-real-time exchange of account and transaction data linked to known fraud, enabling real-time prevention and decisioning.
- **Intelligence Sharing:** Timely, industry-wide sharing of emerging fraud types, trends, and tactics from authoritative sources to help institutions quickly adapt their defenses.
- **Law Enforcement Collaboration:** Coordinated escalation of large-scale fraud cases to law enforcement, shifting from isolated case reporting to systemic investigations aimed at dismantling organized networks.

Legal uncertainty continues to hinder information sharing. Institutions often avoid sharing certain information—even to protect the ecosystem—due to fear of litigation or liability. For example, when suspicious receiver accounts could be linked to first-party fraud, institutions may hesitate to warn peers, concerned it could be construed as triggering FCRA obligations.

While statutes like GLBA Section 313.15, the USA PATRIOT Act’s Section 314(b), and other privacy exemptions permit certain fraud-related sharing, they lack clear safe harbor protections. Section 314(b) in particular is poorly suited for modern fraud collaboration and does not apply to cross-sector sharing with telecom or tech companies—despite their growing role in enabling fraud.

As many banks note, “nothing explicitly prohibits sharing, but nothing clearly permits it either.” This legal gray area results in overly cautious behavior, missed opportunities to disrupt fraud, and unnecessary duplication of effort.

4.1: Establish Safe Harbors and Provide Clear Guidance for Fraud and Scam Information Sharing

The Agencies should work with Congress and other relevant authorities to establish clear legal authority and safe harbor protection for fraud-related data sharing. This includes enabling industries such as social media, telecommunications, and tech companies to share fraud information to protect consumers and reduce fraud. Legal certainty must extend to all parties acting in good faith to protect consumers and the payments system from fraud. To support these efforts, the Agencies can help by reinforcing the importance of robust fraud intelligence functions, much as they have long done with cybersecurity, while allowing banks the flexibility to design programs that fit their risk profile. Regulators can also encourage participation in established information-sharing groups such as FS-ISAC and NCFTA and help remove legal or operational barriers that may limit timely collaboration. The Agencies should support cross-industry efforts to improve fraud data and intelligence sharing across industries, not just within banking.

4.2: The agencies should work with industry to refine the FraudClassifier™ and ScamClassifier™ frameworks

A consistent fraud taxonomy is essential for identifying trends, guiding action, and improving information sharing. The Federal Reserve’s FraudClassifier™ and ScamClassifier™ frameworks are important steps forward, but adoption across institutions has been inconsistent.

These models provide an excellent starting point for standard taxonomies. To enhance and update these models, the Federal Reserve should evaluate integrating emerging frameworks, such as the FS-ISAC Cyber Fraud Prevention Framework³³ or the Fraud Kill Chain³⁴, for more granular attack-stage analysis and mitigation planning. Coordination between industry and agencies to develop a unified, comprehensive

³³ FS-ISAC. (n.d.). [Cyber fraud prevention framework](#). FS-ISAC.

³⁴ Fraud Kill Chain. (n.d.). [Fraud Kill Chain](#).

taxonomy will help advance robust trend analysis and facilitate information sharing. The Agencies should also provide clarity on expectations regarding the use of these models by banks.

4.3: Leverage Suspicious Activity Reports (SAR) to generate more actionable and timely intelligence

In today's digital landscape, fraud attempts, particularly scams, are constant, high-volume, and generate a huge influx of SAR filings. In 2024, over 2.3 million SARs were filed by Depository Institutions related to fraud.³⁵ Banks devote significant time and resources to preparing SARs for fraud cases, creating an administrative workload that diverts resources from customer protection and prevention efforts. Banks receive little feedback on case outcomes, trends, or emerging indicators, that would bolster prevention efforts. This lack of feedback means that SARs function largely as a one-way reporting requirement rather than a collaborative prevention tool.

We recommend the Agencies work with FINCEN to provide feedback on the intelligence generated by these reports. FinCEN should produce and share regular, timely and actionable intelligence derived from SAR data – such as trends, typologies, and indicators – with reporting institutions. Greater dialogue would allow SAR filings to directly inform prevention strategies and support industry collaboration.

The Treasury Department and FinCEN have publicly acknowledged the need to modernize the BSA/AML regime, including SAR reform, to reduce unnecessary burdens and enhance usefulness for law enforcement.³⁶ Recent FinCEN notices and Treasury's Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) National Priorities highlight the importance of improving data quality, streamlining reporting, and increasing feedback to filers. Aligning SAR requirements for payments fraud with these broader reform efforts would ensure that compliance obligations are proportionate to risk and more directly support prevention.

Section V: Reserve Banks' Operator Tools and Services

As the operator of critical payment systems, the Federal Reserve is responsible not only for ensuring system reliability but also for advancing tools that help participants detect and prevent fraud.

The Reserve Banks are uniquely positioned to identify network-level patterns and risks across all participating institutions. The ability for the Fed to share its wide visibility of fraud activity back to the payment system is critical. With that in mind we recommend the following:

- Provide network-wide risk scoring tools based on transaction activity across FedACH, Fedwire, and FedNow, enabling participants to assess the fraud risk of sending and receiving parties.
- Implement standardized fraud reporting for all transactions processed over Reserve Bank platforms to improve data aggregation, trend analysis, and targeted mitigation.
- Require transaction tagging using an agreed classification framework that includes payment flow (C2C, C2B, etc.), use case (eCommerce, bill payment, etc.), and industry segment (retail, financial services, etc.), enabling receivers to manage risk more effectively.
- Support Confirmation of Payee (CoP) across payment types, allowing consumers and businesses to verify recipient information before initiating payments—a proven measure in reducing authorized push payment (APP) scams internationally.

- Facilitate cross-rail fraud detection and insight sharing, especially where fraud typologies migrate between systems (e.g., ACH to FedNow) as tactics evolve.

By embedding these capabilities into the infrastructure it operates, the Federal Reserve can strengthen the security and integrity of its systems while setting a higher standard for fraud prevention across the payments ecosystem.

We appreciate the agencies' leadership and commitment to mitigating fraud in the payments system. Public-private partnership is key to achieving these goals, and we welcome the opportunity to discuss these recommendations further at your convenience.

Please do not hesitate to reach out to the undersigned by email at greg.williamson@bpi.com if you have any questions regarding this letter, or if you would like to discuss further.

Respectfully submitted,

Gregory Williamson

Gregory Williamson
Senior Vice President, Fraud Reduction Program
Bank Policy Institute | BITS



Statement for the Record
of

AARP

On hearing entitled:

Fraud in Focus: Exposing Financial Threats to American Families

before the

United States House Committee on Financial Services
Subcommittee on Oversight & Investigations

September 18, 2025

AARP Point of Contact:
Clark Flynt-Barr, Director of Government
Affairs, Financial Security
(cflyntbarr@aarp.org)

AARP is deeply grateful to the Committee for convening this important hearing, “Fraud in Focus: Exposing Financial Threats to American Families,” and for your leadership in examining the growing threat of scams and financial fraud targeting Americans. This issue is of critical national importance, and we commend the Committee for recognizing the urgent need to explore community, state, and federal strategies to prevent exploitation and protect victims.

Preventing scams and strengthening financial security are core to AARP’s mission. We have long worked to educate consumers, support victims, and improve detection and prevention across industries. We look forward to continuing our collaboration with Congress and federal agencies to advance policy solutions that protect older adults and hold perpetrators accountable.

Fraud in America is at crisis levels. The Federal Bureau of Investigation’s (FBI) numbers show a dramatic increase from the \$800 million in [fraud losses in 2014](#), to 2024, when hardworking Americans had [\\$16.6 billion stolen](#) from them. This is almost a 2000 percent increase in fraud losses over the past decade. And that is likely a very low estimate. In a 2024 [report](#), the FTC estimated the true overall 2023 fraud losses, adjusted for underreporting, was \$158.3 billion for consumers of all ages and \$61.5 billion for older adults.

Transnational organized crime groups are operating openly abroad, [siphoning hard-earned money](#) out of our local communities and economies. These funds—meant for housing, healthcare, and family—are instead lining the pockets of overseas fraud rings. [An AARP study in 2021](#) showed that 9 in 10 Americans encountered a fraud attempt in 2020, and 1 in 7 lost money. Given the steady rise in fraud, even more Americans are likely to report losses in 2025.

Older adults are disproportionately affected, reporting [average losses](#) of \$83,000—more than four times the average loss across all age groups. These crimes often target individuals on fixed incomes, and in some cases, victims lose not just their savings but their homes. One recent case reported to AARP’s Fraud Watch Network Helpline involved a Florida man in his sixties who lost over \$400,000—the proceeds from the sale of his home—to cybercriminals. He went from financial stability to the brink of homelessness in a matter of seconds.

Fraud affects people of all backgrounds. Our Helpline makes clear that scammers do not discriminate based on age, income, geography, or education. And the financial toll is only part of the story—two-thirds of victims report significant emotional or health impacts. The stigma and victim-blaming associated with fraud further compound the harm and discourage reporting, making it harder to understand the true scope of the crisis.

Criminals have professionalized their operations, using advanced technologies and psychological manipulation to exploit victims. It is essential that we shift the narrative to place responsibility where it belongs—on the perpetrators, not the victims. AARP has developed resources to help professionals use trauma-informed language and support victims with compassion and dignity.

Fraud has escalated into a national crisis with profound economic consequences for local communities. These stolen funds, which would otherwise support essential household spending and local economic activity, are instead diverted to transnational criminal groups engaged in drug trafficking, human exploitation, and other illicit operations. International scam hubs,

particularly in Southeast Asia, are profiting at industrial scale, with cyber fraud comprising significant portions of national GDPs. To counter this growing threat, robust consumer protections, regulatory reforms, and coordinated global enforcement are urgently needed.

In this statement, we will highlight AARP's initiatives to combat fraud, including our Fraud Watch Network Helpline, consumer education efforts, as well as the financial and emotional impact of fraud on victims and their families, and the economic impact of fraud on our local communities.

AARP's Fraud Prevention Work

While fraud awareness and prevention has always been a priority for AARP, our fraud prevention work has grown over time as we have heard from our members that fraud is a top concern for them and their financial security. The AARP [Fraud Watch Network](#) was created in 2013, and our fraud prevention work through our state offices has grown significantly in recent years.

AARP works with victims of fraud through our Fraud Watch Network, which offers resources to arm consumers with the knowledge needed to spot and avoid scams. The Fraud Watch Network Helpline is a free resource available to people of any age; you do not have to be an AARP member to use the service. In 2024, the AARP Fraud Watch Network Helpline fielded over 100,000 calls from concerned Americans reporting attempted frauds and scams, as well as those recounting their traumatic experiences of fraud victimization, and the theft of their personal information and/or finances.

For example, just last month, Roger, an 85-year-old, called the Helpline to share his experience. Roger had over \$150,000 stolen from him in a tech support scam. A criminal called him, posing as an Apple representative, and told him the only way "to protect" his money from hackers was to convert and send his money in gold. Another man, Carlos, who is in his 70s, was defrauded by a friend he made in his senior exercise class. This "friend" appears to be part of a network that stole more than \$650,000 from the man. Unfortunately, there are countless more stories just like these. In June of this year, the Helpline received multiple reports from older adults who had formed friendships and romances online with criminals who stole over \$100,000 in each case. These are just a few of the many, many devastating stories our Fraud Watch Network Helpline staff and volunteers hear from older adults every day.

AARP provides extensive community outreach through the Fraud Watch Network and our 53 AARP state offices. [Research](#) shows that consumer awareness about specific scams may reduce vulnerability to those scams by up to 85 percent. To this end, we hold events in communities to raise awareness about different types of fraud and scams. We also partner with law enforcement, regulatory agencies, and Attorneys General to host webinars, tele-townhalls, trainings, and other fraud prevention and awareness events. We have more than 800 volunteers nationwide who deliver fraud education in their communities and work directly with victims of fraud. Each year we reach hundreds of thousands of AARP members and non-members alike from coast-to-coast with our locally driven outreach efforts.

AARP has a Fraud Resource Center and writes extensively about fraud in the [AARP Magazine](#) and [AARP Bulletin](#). Articles and resources include recent fraud news, information about common scams, trends in fraud, and how to recognize and avoid common scams, as well as resources to assist victims of fraud and their families when they encounter scams. We also have [videos](#) that break down how scams work and how to keep yourself safe from criminals. Recent articles have included, “[3 Key Things to Know About Scams in 2025](#)” and “[I Never Thought My Dad Would Become a Romance Scam Victim. Don’t Make My Mistake](#)” and “[SIM Swapping: Scammers Hijack Smartphones and Steal Thousands](#)”. These publications reach millions of Americans and fraud-related articles are some of our most-read and well-received – an indication of how worried our members are about fraud.

AARP launched a weekly podcast called [The Perfect Scam](#) in 2019 to highlight the different types of fraud and scams that we were hearing about from our members and callers to the Fraud Watch Network Helpline. Our host introduces listeners to those who have experienced scams firsthand, as well as leading experts who pull back the curtain on how scammers operate. In December 2023, the *New York Times* [highlighted](#) the scam podcast as a top resource to “deepen your understanding of how liars and con artists operate.” Recent episodes have focused on credit card scams, rental scams, gold bar scams, pet scams, charity scams, time share scams, arrest warrant scams, military benefit scams, romance scams, and job posting scams, among many others. Most of these stories come directly from victims we have worked with on the Helpline who want to share their story to help others avoid similar experiences.

The AARP Fraud Watch Network has also developed a free program to provide emotional support to fraud victims and their friends and relatives. AARP’s [Fraud Victim Support Group](#) provides individuals with an online forum to meet and interact with others who have experienced similar events. Our sessions are a safe environment to give and receive valuable feedback and support from others who are on the road to emotional healing and recovery. Group sessions are confidential and led by trained facilitators who offer fraud education and understanding to participants, as well as time for meaningful peer-to-peer sharing and support. Participants don’t have to be the primary victim of a fraud to participate— family members, partners or friends of a fraud victim are welcome and encouraged to participate. Experiencing fraud can be devastating, and these types of safe spaces can be very valuable to victims and their loved ones in processing and recovering from the trauma it causes.

AARP also runs a program called *BankSafe*, which trains employees at financial institutions to detect fraud and financial exploitation. [BankSafe](#) works with the financial services industry to help them stop financial exploitation *before* the money leaves customers’ accounts. The program encourages those in the financial services industry to voluntarily adopt research-proven interventions, policies, and procedures that effectively prevent exploitation. Researchers from the Virginia Tech Center for Gerontology have [studied](#) the impact of training bank and credit union staff to spot and prevent financial exploitation. In 2018, a [Virginia Tech study](#) with over 2,000 frontline employees in 11 states (including Minnesota and Vermont) found that employees who took the *BankSafe* training saved 16 times more money than those without the training. Based on these findings, we estimate that *BankSafe* policies, interventions, and procedures have, to date, prevented more than \$450 million from being stolen from consumers.

In addition to our fraud prevention awareness, industry collaboration, and victim support services, AARP conducts research on fraud to inform our work and the public at large. According to a 2025 AARP survey on the [Fraud Crisis in America](#) that surveyed American adults (those 18 and older), adults of all ages worry greatly about fraud (37 percent), but this fear is even more pronounced among adults ages 50+ (44 percent). The survey also demonstrated that people continue certain behaviors that put them at a higher risk of becoming the victim of fraud. For example, while most adults reported that they rarely or never answer unknown phone calls, texts, or friend requests, over a third of adults (36%) reported that they usually or always answer one or more of these unknown communications. The survey also looked at how adults were maintaining the security of their devices and online accounts, including the use of VPNs and two-factor authentication, downloading free apps and/or taking online quizzes on social media, and using different passwords on all accounts.

AARP's comprehensive approach to fraud prevention—spanning education, advocacy, direct support, and industry collaboration—demonstrates our steadfast commitment to safeguarding the financial well-being and peace of mind of older Americans. Through continued community engagement, we can work to ensure that everyone is equipped to recognize, resist, and recover from scams—protecting not only personal assets, but also restoring trust and security across our communities.

Victim Experiences of Fraud and Scams

AARP hears directly from victims about the types of scams they are experiencing and how they evolve. We will outline some of the most common types of scams impacting older adults and how they work. Just as the types of scams we see are varied, we see criminals use a variety of different methods to approach their victims, as well as payment methods used to steal their money. Of note, AARP has seen texting, social media, email, phone as the most common venues for criminals to reach their victims as older adults increasingly use text messaging, email, and social media, which makes them increasingly accessible to criminals.

In one example of a scam that started on social media, a woman received a Facebook message from a Brazilian singer she admired who began a long correspondence with her. The woman eventually decided to leave her husband for him. She had given him their life savings — \$300,000 — before learning he was a fraud. Another victim told the Fraud Watch Network that they had been contacted on social media by an account impersonating her friend. They “worked me for 1 year gaining my trust. Then out of the blue, recommended a program called Christian Against Poverty (CAP) that can help with my finances by enrolling me in a grant program from the government. It piqued my interest so I contacted them directly thru Facebook with the recommendation of my “friend.” There, the bad actor told me I can get a lot of money but I needed to send money to be enrolled. So I did. Then the bad actor said don’t tell anyone, not even your family. I mailed the amount of money asked of me. Once cashed, the bad actor stopped responding from CAP messenger and my so-called friend is no longer responding as well. The money went to a rental office in Virginia, the phone number provided to me was someone else’s hacked account, the “pay to” line was an attorney who I suspect is also hacked. They were trying to get my bank info but my son got wind of this secret and stopped it before it got worse.”

Criminals prey on people during times of high stress or need, which makes them vulnerable to becoming a victim. For example, a woman in North Carolina was attempting to leave her abusive husband. She was contacted by someone on social media who promised to “help her” escape. She provided her SSN, bank account, driver's license and paid \$1500 with her debit card (money she was saving to leave). The scammer then disappeared with her information and money. In another case, a 73-year-old woman in Delaware was looking for help for her terminally ill grandson. She was contacted by a “minister” who said he could cure her grandson. She sent him \$110,000 through a payment app to cure him. The “minister” then disappeared with her money.

Computer pop ups continue to be used by criminals, particularly in tech support scams. A 76-year-old woman called the Fraud Watch Network from California. She received a pop-up on her computer from Microsoft. She called the phone number and was told that someone with her information had been viewing and selling child pornography. She gave them access to her computer, her SSN and bank account. They sent someone to her house who drove her to buy \$79,000 in gold coins and also instructed her to send \$21,000 in cash through the mail. They informed her someone else was coming to her home to pick her up and take her to the bank to remove \$400,000 from her retirement account. They texted and called her repeatedly and scared her.

Another victim, 76-year-old woman in California, received a pop-up on her computer from Microsoft. She called the phone number and was told that someone with her information had been viewing and selling child pornography. She gave them access to her computer, her SSN and bank account. They sent someone to her house who drove her to buy \$79,000 in gold coins and also instructed her to send \$21,000 in cash through the mail. They informed her someone else was coming to her home to pick her up and take her to the bank to remove \$400,000 from her retirement account. They texted and called her repeatedly with threats.

Payment methods like gift cards remain very popular with criminals. In one example, a victim told AARP that Health and Human Services agents called them and claimed they had hundreds of thousands dollars awarded to me. In order to collect the alleged “award”, the “agents” “claimed all kinds of charges like delivery charge, safe purchases, issues with paperwork not being completed, imposter tried to collect my money, IRS certificate money needed, payment for PCV and insurance and on and on. [They even sent] photos of the FedEx delivery truck being stopped by ATF. I paid in Apple Gift cards in the amount of \$22,000. This has been an 8-month ordeal. I never received a cent. They still owe me for 3 safes that said they needed to purchase to deliver the money in.”

Criminals adapt to new technologies and AARP has seen a large increase in cryptocurrency as the requested payment method. Cryptocurrency is more widely accessible, but not widely understood, and there has been a lot of “buzz” around it in recent years. It is also easier to move large quantities of money quickly via cryptocurrency than other assets, including via cryptocurrency ATMs, which allow people to insert cash and then send cryptocurrency to a digital wallet address (in the case of scams, to the wallet of a criminal). One victim told AARP, “A friend of mine who said she lives in Boston introduced me to [website]. Over several weeks, I transferred 85,000 to this company. My returns were significant. Currently, my “balance” is

\$230,273.70. When I tried to do a withdrawal, I was stopped by the website. They said I needed to give them 38000 for capital gains taxes. I then did further research. My brother is an attorney, and he determined that they were a pig butchering site.”

Another cryptocurrency investment scam victim, an 84-year-old man in Minnesota, lost millions in a cryptocurrency scam. He was forced to sell his house and became estranged from his sons who tried to tell him he was being scammed. In what is becoming increasingly common, the victim was re-victimized in a “recovery” scam. After he learned the fraud had occurred, the man received a call from someone claiming to be a “hacker” who could get his money back. He sent him \$400,000 to retrieve his money but hasn’t heard from the hacker since. He still believes he can get his money back and that his family will forgive him.

A recent Helpline case using cryptocurrency involved a 69-year-old Greenfield, Ohio, woman who started a romance online with a gentleman who said he was an American architect in Cape Town, South Africa. He told her he was stuck there because his investors were late paying him on a building project. He provided a LinkedIn profile, and a copy of his passport. She opened a bank account that he wanted her to use to convert his funds into crypto when he received them. She became suspicious that this was a scam when she tried to verify that he was in fact a licensed architect in Massachusetts as he had claimed and was not able to. Our Helpline volunteers helped her compile a complete report that she could send to law enforcement and helped her identify where to report the crime.

Celebrity impersonation cases continue to also be quite common. A Nevada resident called the Helpline to report their neighbor was being defrauded. “He was contacted initially on Facebook by someone claiming to be Elon Musk and has sent thousands (I don’t know the exact amount) in Apple gift cards to these varmints. The criminals have promised him a new Cybertruck that has been “on its way” to him at least seven times since this started right after the election. It would be here, but “customs” keeps holding it at state lines in AZ, NM, and TX. They have also sucked thousands out of him to “invest” in Tesla stock which will supposedly grow into a fortune because of this “insider information.” Tonight, I saw him send his entire monthly Social Security to this criminal (\$2500) in Apple cards... The phone number he’s talking with is a Nigerian number.”

Magis, who reached out to AARP’s Fraud Watch Network, experienced a complex bank impersonation scam and was made to believe that her bank’s fraud investigators were seeking to help her address fraud in her accounts. They told her that her stolen identity was being used by foreign cybercriminals who used it to buy child sexual exploitation materials, murder people, and sell body parts. The impact grew to affect her retirement account, and more than \$1 million was stolen throughout the scam. She faces a substantial loss of Social Security retirement benefits due to the withdrawals from her retirement accounts, which put her income in the highest withholding category. Magis has suffered significant stress and faces the possibility of losing her home and becoming homeless.

Kate, a suburban Philadelphia widow did not plan to date again until a handsome “surgeon” asked to be her Facebook friend. Soon “Tony” became romantic and professed his love. Though the two never met in person, Tony talked about marriage, said he purchased a ring and asked her

to look for a house for them near where she lived. All the while, he kept prodding her for gift cards — and promising he'd repay her. He even provided her with a password for a purported bank account with a \$2 million balance. The two were to meet for the first time in December 2020; he said he'd fly to Philadelphia International Airport. She had her hair and nails done and waited at home in her best dress for his call. A bottle of wine was chilling. Hours passed, without a word from him. A day later, Kate got a call from a man who claimed to be a lawyer saying Tony had been arrested at the airport because someone planted drugs in his luggage. Tony was said to be confined to a Philadelphia jail and needed \$20,000 for bail— money she did not have. Later, Tony called and messaged to urge her to get the money somehow, even if it meant lying to her family. She refused. But her reservations melted away when he complained about the “awful” food in jail and asked for small sums, which she sent. Then Tony's story got even more improbable. He called saying he was in Jordan; he said he'd been released so he could raise the bail money. She said that wasn't the way it worked: You don't get out of custody to raise bail. Finally, she saw the romance for what it was — phonier than a \$3 bill. Though Tony was fake, her heartbreak was real. What hurt most, she said, was “losing his love and losing the family I thought I was going to have and what my new future was going to be... That is much harder to deal with than losing the money.” She ended up losing everything she owned — including her home — in the coldhearted scam that played on her emotional vulnerability and kindness.

Financial and Emotional Impact of Fraud on Victims

Through our initiatives with the Fraud Watch Network, AARP frequently hears directly from victims about the profound effects fraud has had on their lives. These individuals recount how scams have caused financial devastation and emotional turmoil, highlighting the severe consequences of such crimes. Family members share the ripple effects on their households. Our work also reveals the emotional toll on first responders and victim service providers who assist these victims. Fraud significantly impacts our communities, and it is crucial to understand its various effects.

This financial loss can result in greater reliance on credit cards, which can lead to debt and impact the victim's credit score, making it more difficult for them to obtain loans, mortgages, or rent an apartment. Victims may lose their home and be forced to move in with family members or friends. They may become reliant on social safety nets, and this can strain community resources. Victims have reported that where their retirement accounts have been drained by criminals, this has affected their Social Security benefits, as retirement account withdrawals can result in higher income brackets and greater taxes on both their lost retirement funds and their benefits.

There are also serious emotional ramifications of fraud. Victims report feeling frustration, anger, mistrust, and sadness after experiencing fraud — and some unfortunately commit suicide. According to a FINRA [study](#), two-thirds of fraud victims reported experiencing at least one non-financial cost of fraud to a serious degree. These included severe stress (50%), anxiety (44%), difficulty sleeping (38%), and depression (35%). Victims who lose more money are more likely to incur more non-financial costs. These emotional impacts of fraud often lead victims to not report that crimes have been committed against them because of the guilt and shame they may

feel. This contributes to significant underreporting to law enforcement, resulting in an unclear picture of the true scope of the problem and where to focus investigative efforts.

Despite growing awareness of financial fraud, our societal response often compounds the harm victims experience. AARP's June 2022 report, [Blame and Shame in the Context of Financial Fraud](#), highlights how language in media and everyday conversation subtly blames victims—phrases like “duped” or “fell for it” suggest culpability and diminish the seriousness of the crime. This framing not only discourages victims from reporting fraud but also isolates them emotionally. According to the report, while 85% of Americans believe fraud can happen to anyone, over half still view victims as blameworthy. Such attitudes reflect cultural biases, including assumptions about older adults being less tech-savvy or cognitively impaired, even though data shows younger adults report fraud more frequently. The emotional manipulation used by criminals is sophisticated and deliberate, often triggering victims to make decisions based on trust and urgency rather than logic.

Changing how we talk about fraud is not just a matter of compassion—it's a matter of justice. When scams are treated like the crimes they are, victims are more likely to report them, law enforcement is more likely to act, and prosecutors are more likely to pursue cases. AARP's report calls for a shift in narrative: replacing headlines like “Americans Swindled in \$13M Wine Investment Scam” with “Criminal Stole \$13 Million in Wine Investments” reframes the issue from victim error to criminal intent. Victims deserve empathy, not judgment. As one former prosecutor noted, the emotional toll of fraud can be so severe that some victims “move into a state of depression that they can't ever get out of.” By ending the cycle of shame and blame, we can better support victims, strengthen family relationships, and ensure fraud is recognized and prosecuted as the serious crime it is.

HERE ARE EXAMPLES OF WHAT TO SAY:

INSTEAD OF THIS:

How could you fall for that?

SAY THIS:

This isn't your fault — you experienced a crime.

INSTEAD OF THIS:

How much money did you give them?

SAY THIS:

How much did the criminal steal?

The story of one victim who reached out to the Helpline, Mo, does a good job of highlighting the emotional impact of fraud. Mo was the victim of a devastating investment scam that resulted from meeting someone online who eventually convinced him to invest in cryptocurrency. The criminals involved stole millions from Mo and his family. He continues to beat himself up for the damage this has caused to his marriage and his two children. He has suicidal thoughts, but

also realizes he needs to be around for his family. He constantly asks himself, “how could I be so dumb and stupid?” This is unfortunately a very common experience for fraud victims.

In another story, a Los Angeles woman talks about the impact of being targeted by a criminal impersonating a TV journalist she admired. She had sent him a message telling him she liked his work when she found his social media profile online. In the end, the criminal impersonator stole \$70,000 from her via wire transfer, gift cards, and Bitcoin. She was left with \$500 to buy groceries and pay her bills. She said, “I’m crying every day. I don’t know what to do. And I’m taking money out of my retirement and my savings that I had saved for years.” At one point her thoughts turned suicidal. She drove herself to a hospital, where she was quickly admitted. When she told the psychiatrist on duty her story, he said, with sympathy, “You’ve been scammed.” She’s been dealing with the emotional fallout ever since.

Fraud support services are an important component in helping victims process and recover from fraud. AARP’s Fraud Watch Network serves a very important role for victims, as one of the few resources with people willing to listen and help victims process what has happened to them, as well as help them report the crime. Many of the victims share with our Helpline volunteers that they have no one in their lives who will understand what is happening and they are embarrassed to talk to them about it. We cannot allow victims’ horrible experiences to leave them alone and isolated. More than anything, they need support – and until families and friends understand this, AARP and other victim support groups will be there to help them recover. Not only do we need to focus on victim support, but we must support families too. We hear from many families that even when they are supportive and compassionate to their loved ones, they themselves have significant guilt or confusion on why this happened. We hear from grandchildren whose grandparents have been a victim of a grandparent scam have survivors’ guilt and need support. Understanding the emotional impact of fraud is critical to changing how we respond to victims.

The ripple effects of fraud can destabilize entire households. Promises to help children or grandchildren financially may be broken, and retirement plans may be derailed. Some family members take on debt or postpone their own retirement to support the victim, while others face emotional fallout, including anger, shame, and isolation. Many scam victims over age 60 report relationship problems with friends or family as a result. Experts emphasize the need to break the silence surrounding scams. Open dialogue, victim support groups, and family counseling can help relatives process their emotions and avoid blaming the victim.

Carisa K. shared how her 73-year-old mother lost \$300,000 in a sophisticated help desk scam. The funds had been earmarked for family support—home down payments and college tuition for grandchildren—but were instead stolen through emotional manipulation and deceit. Carisa, a costume designer in New York, spent hundreds of hours trying to recover the money and manage the fallout, including the possibility that her mother may need to sell her home to cover tax liabilities. This story is emblematic of a broader trend: a [2023 Gallup poll](#) found that 15% of Americans had a household member deceived by a scam in the previous year—more than those affected by theft or burglary.

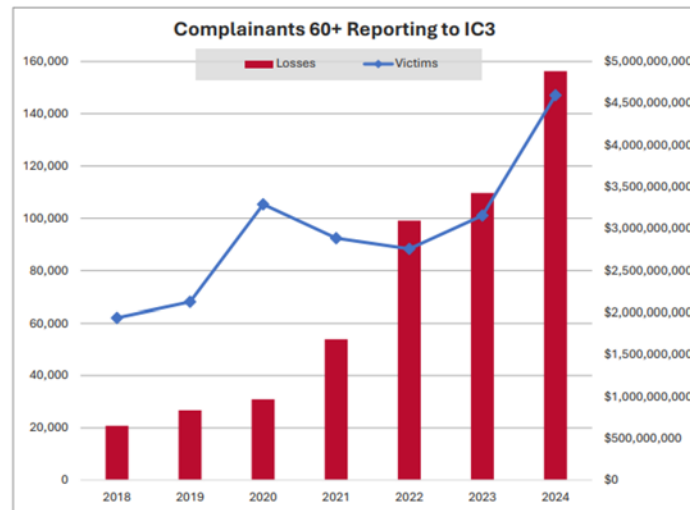
Criminologists and psychologists note that family members often become “secondary victims,” experiencing emotional strain, financial loss, and disrupted relationships. When scams strike,

adult children may find themselves suddenly responsible for their parents' finances, care, and emotional well-being. In another case, Rory M. discovered that his dying mother had been victimized by multiple romance scams totaling \$800,000. The secrecy surrounding the fraud robbed him and his sister of the chance to say a proper goodbye. Instead of spending her final days in peace, the family was consumed by confusion, legal paperwork, and emotional distance. Rory later joined a support group and came to understand that his mother wasn't at fault—her money was stolen, and the weapon was emotional manipulation.

Economic Impact on America's Local Communities

Fraud is not merely a personal tragedy—it is a national crisis. It undermines the safety and security of our citizens and erodes the economic vitality of our neighborhoods. The consequences are far-reaching, affecting individuals, families, and the broader systems that sustain our society.

According to the FBI, reports from Americans 60-plus have increased since 2018, and losses have unfortunately skyrocketed.



According to FBI data, reports of fraud targeting Americans aged 60 and older have increased dramatically since 2018. According to the Federal Bureau of Investigation, reports of fraud targeting Americans aged 60 and older have increased dramatically since 2018. In 2024, the average reported loss for a victim over the age of 60 was \$83,000. This represents a staggering increase from 2020, when the average loss was \$9,175. These figures, while alarming, are widely understood to be massive underestimates. Experts estimate that the true financial losses may be ten times higher than what is reported.

The impact on our local communities and their economics is dramatic. The average older fraud victim has more stolen from them than they would spend on utilities, medical care and medication, groceries, housing, and tithing in *two full years*. This is money that would otherwise circulate within our communities—supporting small businesses, funding local services, and contributing to economic growth. Instead the funds are siphoned off into the hands of transnational organized crime, who use the money for [drug operations](#), [human trafficking](#), and other illicit activity.

The international dimension of this crisis is equally disturbing. According to the U.S. Institute for Peace, cyber scamming operations in countries such as Cambodia, Laos, and Myanmar have reached industrial scale. According to [the U.S. Institute for Peace](#), some countries harbor so much scam activity that it makes up sizeable portions of their gross domestic product: *“In Cambodia, the return on cyber scamming is estimated to exceed \$12.5 billion annually—half the country’s formal GDP—with many compounds owned by local elites. More broadly, the study group calculates that the funds stolen by these criminal syndicates based in Mekong countries likely exceeds \$43.8 billion a year—nearly 40 percent of the combined formal GDP of Laos, Cambodia, and Myanmar. A significant share of these profits is reported to flow to the Myanmar military and to ruling elites in Cambodia and Laos.”*

As technology continues to evolve, so too must our defenses. We must establish robust safeguards to protect consumers, maintain confidence in our financial systems, and ensure that emerging technologies are used for legal and ethical purposes. This includes stronger regulatory frameworks, enhanced public education, and coordinated international efforts to dismantle fraud networks at their source.

Conclusion

AARP thanks Subcommittee Chairman Meuser, Ranking Member Green, Chairman Hill, Ranking Member Waters, and all Members of the Committee for your leadership in shining a light on the devastating impact of financial fraud on American families. As this hearing has made clear, fraud is not only a personal tragedy—it is a systemic threat to our national and economic security. Older adults are disproportionately targeted, and the ripple effects of these crimes destabilize households, drain community resources, and fuel transnational criminal networks. AARP remains committed to working with Congress, federal agencies, and community partners to advance meaningful solutions that protect consumers, support victims, and hold perpetrators accountable. We urge continued investment in prevention, enforcement, and victim support, and we stand ready to collaborate on policies that restore trust, dignity, and financial security for all Americans.



September 18, 2025

The Honorable Dan Meuser
Chairman
Subcommittee on Financial Institutions
House Financial Services Committee
Washington, DC 20515

The Honorable Al Green
Ranking Member
Subcommittee on Financial Institutions
House Financial Services Committee
Washington, DC 20515

Dear Chairman Meuser and Ranking Member Green:

On behalf of the American Financial Services Association (AFSA),¹ thank you hosting a hearing entitled, "Fraud in Focus: Exposing Financial Threats to American Families." We appreciate the Financial Services Committee for highlighting how different types of financial fraud and scams are affecting American families and businesses at alarming rates.

Credit Repair Scams

As part of the 119th Congress, we urge the Committee to pass H.R. 306 - Ending Scam Credit Repair Act (ESCRA). This is bipartisan legislation will help protect consumers from fraudulent credit repair organizations (CROs) practices and prohibit these entities from "jamming" financial institutions with duplicative credit dispute requests. Unfortunately, we have seen a rise in CROs using generic form letters to dispute negative items on credit reports, regardless of accuracy, to flood lenders and divert our resources away from legitimate consumer disputes. ESCRA would help improve the consumer lending markets and help alleviate stress on the dispute process for financial service providers, including small business lenders.

Debt Settlement Industry Shady Practices

For far too long, the for-profit debt settlement industry has been rife with entities claiming to provide consumers with a quick way of settling existing debts at a fraction of the cost. In reality, debt settlement companies can leave consumers worse off than they started by misleading consumers to stop paying their lenders all while damaging their credit score, charging enormous fees, and potentially paying more in taxes.

Unfortunately, the debt settlement industry lacks sufficient regulation at the federal level and continues to target financially vulnerable consumers and consumers in good standing with an

¹ Founded in 1916, 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.

average of \$26,000 in debt.² Both federal agencies and state financial regulators across the country have issued warnings for consumers about these types of scams.³

We encourage the Committee to modernize debt relief regulations to protect consumers and financial institutions operating in the marketplace from shady practices occurring in the for-profit debt settlement industry.

Auto Loan Fraud

In 2025, auto lenders will lose an estimated \$9.2 billion in fraud – the highest ever measured, according to recent reports.⁴ Driven by AI tools, synthetic identity theft, credit washing methods, and others, auto-related fraud is rated as a top category according to the Federal Trade Commission's Consumer Sentinel Network.⁵

These scams raise costs for lenders and ultimately harm the entire automobile retail ecosystem, including law-abiding consumers. Moreover, the high costs involved in combatting fraudulent activity threaten to drive smaller-scale financial institutions out of the auto financing industry altogether, potentially reducing competition in the marketplace.

As Congress discusses different financial frauds and scams, we encourage the Committee to work with relevant federal agencies to examine potential solutions addressing the increase of auto fraud activities.

Thank you for conducting this hearing and we stand ready to work with you on these important issues affecting consumers and businesses. If you have any questions, please contact Ann Harter at (202) 466-8606 or aharter@afsamail.org. We appreciate the opportunity to comment before this hearing.

Sincerely,



Celia Winslow
President and CEO
American Financial Services Association

² [Freedom Debt Relief \(September 6, 2025\)](#)

³ [FTC: Debt Relief Service and Credit Repair Scams](#)

⁴ [Point Predictive: 2025 Auto Lending Fraud Trends \(March 25, 2025\)](#)

⁵ [FTC: Top Scams of 2024 \(March 10, 2025\)](#)



September 25, 2025

The Honorable Dan Meuser
Chairman
Subcommittee on Oversight and
Investigations
Committee on Financial Services
U.S. House of Representatives
Washington, DC 20515

The Honorable Al Green
Ranking Member
Subcommittee on Oversight and
Investigations
Committee on Financial Services
U.S. House of Representatives
Washington, DC 20515

**Re: U.S. House Financial Services Subcommittee on Oversight and Investigations
Hearing on “Fraud in Focus: Exposing Financial Threats to American Families”**

Dear Chairman Meuser and Ranking Member Green,

The Securities Industry and Financial Markets Association (“SIFMA”) commends the House Financial Services Subcommittee on Oversight and Investigations for holding this important hearing to examine the rise of financial fraud and its impact on American families. Fraud targeting seniors and vulnerable investors is one of the fastest-growing threats to our financial system, and we value the Subcommittee’s leadership in exploring how federal agencies can better mobilize existing authorities 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 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.

Because financial fraud has a disproportionate impact on seniors — who are among the most targeted investors and control the largest share of financial assets — SIFMA supported the 2018 [Senior Safe Act](#), which provides immunity from liability in civil or administrative proceedings for financial professionals who report suspected financial



exploitation of a senior. We also strongly support [the Financial Exploitation Prevention Act](#), which recently passed out of the House Financial Services Committee unanimously and would authorize mutual funds to place temporary holds on suspicious transactions, the same authority FINRA has already extended to broker-dealers. We commended the bipartisan efforts behind this bill and urge its swift enactment. Lastly, SIFMA supports the [Senior Security Act of 2025](#), which would establish a Senior Investor Task Force at the U.S. Securities and Exchange Commission ("SEC") and passed the House in July.

Our commitment to investor protection extends beyond legislative advocacy. SIFMA works closely with federal and state securities regulators, law enforcement, victim support services organizations, research institutions, and other nationwide partners. In June, we co-hosted a [webinar](#) with the National Adult Protective Services Association ("NAPSA") on World Elder Abuse Awareness Day, which featured panels on recognizing and identifying solutions to address undue influence and how AI is used to both help prevent and perpetrate fraud and scams. We also recently 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.

As noted above, SIFMA has established strong partnerships with law enforcement, including the U.S. Department of Justice, U.S. Postal Inspection Services, FBI field offices, and local authorities to create a multi-disciplinary approach to addressing scams and fraud. Additionally, we have collaborated with researchers and institutions such as Stanford, Yale, the University of Iowa, Hunter College, and more to better understand the scale and scope of financial fraud and strengthen the evidence base for prevention and intervention strategies.



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.

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



Capital One
1600 Capital One Drive
McLean, Virginia 22102

September 11, 2025

The Honorable Zach Nunn
United States House of Representatives
1410 Longworth House Office Building
Washington, DC 20515

The Honorable Josh Gottheimer
United States House of Representatives
203 Cannon House Office Building
Washington, DC 20515

The Honorable Scott Fitzgerald
United States House of Representatives
2444 Rayburn House Office Building
Washington, DC 20515

Dear Congressman Nunn, Congressman Gottheimer, & Congressman Fitzgerald,

On behalf of Capital One, I am writing to express our strong support for your legislation, the "Guarding Unprotected Aging Retirees from Deception (GUARD) Act." We appreciate your focus on finding solutions for combatting financial crimes targeting American seniors and applaud your leadership on this important matter. Criminal scams and fraud, increasingly perpetrated by foreign state actors and global crime syndicates, have vast financial implications not only for their victims but also for the broader U.S. economy, by eroding trust and confidence in our financial system. Ahead of the upcoming House Financial Services Committee hearing on this topic, we are pleased to endorse your bipartisan bill and to share some additional perspective as you prepare for a fruitful discussion.

At Capital One, we believe everyone deserves to feel confident and in control when it comes to their money. A core component of that is our steadfast commitment to protecting our customers from being exploited by financial criminals. We are continually investing in new technologies and layered defenses, real-time transaction monitoring and targeted interventions to short-circuit criminal scammers and protect our customers. We supplement that work with customer education campaigns, by partnering with law enforcement agencies and, as always, providing zero liability for unauthorized transactions in a policy that goes above and beyond what is required under federal law.

Importantly, we know that no single entity or industry has the capabilities to disrupt the criminal enterprises that are perpetrating scams and fraud alone. It is for this reason that we support the GUARD Act. Sophisticated criminal networks are waging a multi-front war against the American consumer—not just within the payments system but across every mode of modern communication and commerce. By uniting government, law enforcement and the private sector



Capital One
1600 Capital One Drive
McLean, Virginia 22102

to craft multi-sector solutions, the GUARD Act represents a meaningful step forward in addressing this critical challenge.

In our own business, we have long understood the critical need for cross sector partnerships for addressing the broader threat landscape. That was the impetus behind our decision to join the Aspen Institute's National Task Force for Fraud & Scam Prevention, an effort launched last year to galvanize action and information sharing across industry, government, and law enforcement. Capital One has also partnered with the Better Business Bureau (BBB) Institute for Marketplace Trust on critical consumer education campaigns, including the launch of the BBB Scam Tracker to help consumers better identify and report scams. In partnership with the BBB and Amazon, we introduced the Scam Survivor Toolkit to provide personalized recovery plans to scam survivors. Capital One also has a longstanding partnership with the education nonprofit Khan Academy, focusing on helping individuals become financially empowered through a free online financial literacy course.

We have seen the effectiveness of cross sector partnerships in surfacing solutions firsthand, but we also believe more is needed to ensure we can effectively address fraudulent financial activity. The scale and accelerating level of sophistication of financial scams targeting not only seniors but all Americans is alarming, and new solutions are needed. The current response to scams is fragmented, with government agencies, financial institutions, telecom and social media companies often working in silos. That is why, in addition to endorsing the GUARD Act's provisions for protecting older Americans, we are calling for greater public-private collaboration to combat criminal scammers across all populations. We believe our work with telecom providers to prevent spoofing of Capital One phone numbers is an illustration of what is possible when industries work together to prevent scams:

- Up until the past year, there was no way to protect our own Capital One phone number from being spoofed by scammers looking to take advantage of customers' implicit trust conveyed by a purported bank-owned phone number showing up on the Caller ID. After years of discussion with telecommunications carriers, there are finally new, fee-based services available for addressing this issue. We now use this new service to protect Capital One-owned phone numbers from being spoofed by scammers and on an annualized basis, we have blocked more than five million spoofing attempts against our toll free numbers, branch numbers, and cafe numbers.
- While this is a step in the right direction, we also recognize the limitations of these developments including the inability to prevent spoofing of text messages and swiftly bringing these bad actors to justice.



Capital One
1600 Capital One Drive
McLean, Virginia 22102

While our efforts to prevent spoofing of Capital One's phone number is a step in the right direction, we also recognize the limitations of these developments including the inability to prevent spoofing of text messages and swiftly bringing these bad actors to justice. As the threat environment evolves—and as the malicious actors driving these crimes become seemingly more innovative, determined and well-resourced—one thing has become abundantly clear: no single institution or industry has the capabilities to unilaterally address this problem. Again, we applaud The GUARD Act and its bolstered measures to strengthen the resources available to law enforcement as they investigate these financial crimes. Ensuring those on the front lines working to bring justice to victims, capture criminals and prevent further harm is imperative.

We believe the GUARD Act would unite law enforcement, the government and the private sector to create multi-sector solutions to take on illicit actors. Capital One remains committed to continuing our partnerships with law enforcement and across sectors to address this critical challenge and we are grateful for your leadership on this matter. We stand at the ready to lend our expertise to the policymaking discussion around combating criminal scams and fraud, and we are hopeful for swift consideration and passage of the GUARD Act.

Sincerely,

A handwritten signature in black ink that reads "Emily Weems".

Emily Weems
Head of Global Policy Affairs Group (GPAG)
Capital One

Cc: The Honorable French Hill
The Honorable Jim Jordan

The Honorable Maxine Waters
The Honorable Jamie Raskin



October 14, 2025

Chairman French Hill
House Committee on Financial Services
2129 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Hill:

Enclosed are my responses to the questions for the record submitted following the September 18, 2025 hearing in the Subcommittee on Oversight and Investigations of the House Committee on Financial Services titled "Fraud in Focus: Exposing Financial Threats to American Families."

Thank you for the opportunity to testify, and please let me know if I may be of any further assistance.

Sincerely,

Paul Benda
Executive Vice President, Risk, Fraud, and Cybersecurity
American Bankers Association



Questions for Paul Benda

From Rep. Williams (GA):

What do you say to consumers who the banking industry has failed and who have relied on the CFPB as a final course of action when all else has failed them?

Thank you for the question, Rep. Williams. As noted in my testimony, banks have long been on the front lines of protecting consumers from fraud, from chip-enabled cards to multi-factor authentication, from AI-driven fraud detection to real time alerts. The banking industry has invested billions of dollars to make our financial system one of the most secure in the world, and Americans recognize that effort. Surveys show that nine out of ten customers say their bank is taking proactive steps to protect them from fraud.

But criminals are innovating too. They've reinvested the \$300 billion stolen during the pandemic to build highly organized networks that now use deep fakes, spoofed caller IDs, stolen checks, and fake social media accounts to target Americans.

This is where banks face a critical limitation. By the time a victim is ready to send a payment, they often believe they know and trust the scammer. Caller ID might display the bank's name. A text message might look identical to a legitimate fraud alert. A social media ad might appear to come from a trusted company. These tools are outside of a bank's control, which is why the banking industry cannot fight this battle alone.

Other stakeholders must play a more significant role in combatting fraud. Telecommunication companies must stop criminals from impersonating banks through spoofed phone calls and fraudulent texts. Today, a criminal overseas can make a call appear as if it's coming from a number on the back of your debit card, a deception tactic that makes it appear as if the call is coming directly from a consumer's bank. In addition, social media platforms must remove fake accounts and fraudulent ads more quickly. The Wall Street Journal recently documented how fake investment promotions on Instagram and Facebook have cost consumers their life savings. Banks regularly flag these scams, but removal of these fake promotions is often slow and inconsistent. Further, the postal service must strengthen protections against check theft, which remains one of the fastest growing forms of fraud. Also, law enforcement needs more resources to investigate and prosecute cases, because no amount of bank investment can replace the deterrence of criminal prosecution.

We urge Congress, the administration, regulatory agencies, and others in the private sector to help close these gaps.

- First, the administration should create a White House Office of Fraud and Scam Prevention to coordinate federal efforts, unify consumer reporting, and drive a national strategy.



- Second, we should require telecom accountability by closing loopholes that allow spoof calls and texts. It's critical that we take steps to ensure caller ID cannot be faked and ban SIM boxes that send thousands of scam texts.
- Third, we must make sure social media companies are included in these fraud protection efforts by mandating quick, free removal of impersonation accounts and imposing liability on platforms that knowingly allow them to remain.
- Fourth, we must support law enforcement by providing for state level financial crimes units modeled on Texas' Financial Crimes Intelligence Center, which has proven effective at coordinating law enforcement investigations for various types of organized financial crimes.
- Fifth, we need to improve information sharing by creating safe harbors for banks and regulators to exchange fraud data and require the Federal Communications Commission to establish a searchable spam text and messaging database.
- Finally, we need to continue to combat check fraud by supporting the development of a national check verification system to authenticate checks at deposit.

Banks are proud of the role we play in protecting consumers, and the banking industry continues to invest, innovate, and educate. ABA has launched several national anti-fraud campaigns, including “#BanksNeverAskThat” and “#PracticeSafeChecks” to help people recognize scams, as well as Safe Banking for Seniors to help combat the ever-growing problem of senior fraud. But unless every player in the fraud ecosystem accepts the responsibility of working toward shared solutions, criminals will continue to victimize Americans at an unprecedented scale. Fraud is not just a banking problem, it is an ecosystem problem, and until all parts of that ecosystem are equally committed to protecting consumers, the American public will remain at risk.

Written Answers to Questions for the Record
 From Kate Griffin, Aspen Institute Financial Security Program
 For U.S. House of Representatives, Committee on Financial Services
 Sub-committee on Oversight and Investigations
 Hearing titled: "Fraud in Focus: Exposing Financial Threats to American Families"

September 18, 2025

Question from Representative Nikema Williams:

- **What do you say to consumers who the banking industry has failed and who have relied on the CFPB as a final course of action when all else has failed them?**

Thank you for your important question and your continued advocacy on behalf of consumers who have been left to fend for themselves when fraud or scams occur. We share your concern for protecting them and agree that Americans deserve fair and effective safeguards that help ensure the safety and trustworthiness of electronic systems, which they use every day to communicate and transact.

The Consumer Financial Protection Bureau plays a valuable role in safeguarding consumers and their financial well-being. Unfortunately, the scams crisis has grown far greater than the remit of any single agency. The scams epidemic has spread, threatening not just finance but also virtually all our systems of electronic commerce and communication, including social media and advertising. In this sense, the CFPB cannot, nor should be expected to, carry the entire burden of protecting Americans from scams. Our work at the Aspen Institute Financial Security Program and the National Task Force on Fraud and Scam Prevention, which we convened, found that the scams crisis demands a whole-of-government and whole-of-society response, one that mobilizes law enforcement, intelligence, financial institutions, technology and communications platforms, community organizations—and yes, the CFPB, FTC, FCC, and their federated regulators—to work together. Their combined mission should be to stop scams before they occur and ensure a more effective process of recovery for those who become victims.

We believe that it is critical to focus effort on protecting consumers by making scams harder to execute, less profitable, and riskier for criminals. That means, among other things:

- Modernizing law-enforcement and data exchange systems so that scam reports lead to faster investigations and recoveries;
- Creating a single, easy-to-use national reporting portal so that both companies and individual victims can report scam activity and, where needed, get help from the right agencies, quickly;
- Incentivizing and empowering companies across banking, telecommunications, and digital platforms to act confidently against scammers—supported by clear rules and legal "Good Samaritan" protections; and
- Elevating scam prevention as a national priority with clear leadership, dedicated funding, and public accountability.

No one—and certainly, not the most vulnerable among us—should be left alone to defend themselves against the sophisticated, transnational criminal organizations that are scamming and harming Americans every day. Already, one in five U.S. adults (approximately 53 million Americans) have lost money to such criminals.¹

By aligning public and private efforts, and with dedicated whole-of-government leadership, we can ensure that Americans benefit from stronger defenses before fraud occurs and a more coordinated system to help when it does.

¹ Jeffrey Gottfried, Eugenie Park, and Monica Anderson, "Online Scams and Attacks in America Today." Pew Research Center, July 31, 2025. <https://www.pewresearch.org/internet/2025/07/31/online-scams-and-attacks-in-america-today/>



NATIONAL HEADQUARTERS
7 Winthrop Square, Boston, MA 02110
(617) 542-8010

WASHINGTON OFFICE
Spanogle Institute for Consumer Advocacy
1001 Connecticut Avenue, NW, Suite 510
Washington, DC 20036
(202) 452-6252

NCLC.ORG

November 19, 2025

Mr. Svent Bossart, Clerk
House Financial Services Committee
Svent.Bossart@mail.house.gov

Re: Response to Question from Representative Nikema Williams regarding the
September 18, 2025, hearing titled "Fraud in Focus: Exposing Financial Threats to
American Families."

Representative Williams,

Thank you for your question and interest in protecting consumers from fraud. You asked:

What do you say to consumers who the banking industry has failed and who have relied
on the CFPB as a final course of action when all else has failed them?

There is not much we can say, other than we are deeply troubled by the many measures
undertaken to weaken the CFPB and, as a result, deprive consumers of a federal agency tasked
primarily with protecting consumers.

There are other stopgap measures consumers can take, but even these measures have proven
insufficient. We steer low-income consumers who have been impacted by payment fraud to legal
services organizations, but these are woefully understaffed and underfunded. Many consumers
cannot afford private attorneys or may not even have legal recourse. State and local law
enforcement agencies, including local police departments, are also understaffed and
underfunded, and as such, most often do not prioritize cases involving fraud, especially when
they lack sufficient training to pursue the stolen funds that have been sent internationally or have
been converted to cryptocurrency.

As my testimony and that of the other witnesses revealed, billions of dollars are lost annually due
to fraud, and consumers are not positioned to bear the brunt of the financial cost associated with
fraud. The CFPB was actively working on addressing fraud, but is now in tatters. Congress

House Financial Services Subcommittee on Oversight and Investigations
“Fraud in Focus: Exposing Financial Threats to American Families.”
September 18, 2025

blocked the CFPB from supervising P2P apps, which would have helped fraud victims. With a change in leadership, the CFPB dismissed various enforcement actions that would have helped fraud victims. Two such examples were an enforcement action involving fraud on Zelle and another enforcement action against Comerica for the obstacles many fraud victims faced when trying to avail themselves of EFTA protections associated with their Direct Express account. Although the New York Attorney General has filed a similar suit against Early Warning Services for failure to prevent and address fraud on Zelle, only impacted consumers in New York will benefit from such an enforcement action. Consumers all over the country need to be protected and made whole when unsafe payment systems are exploited by bad actors.

This is not the time to weaken the Agencies tasked with protecting consumers. The current Administration's actions gutting the CFPB have not only violated the duties imposed by the Dodd-Frank Act but have also left consumers across the country at the mercy of unscrupulous actors. We need all hands on deck to fight fraud, including restoring the strength of the CFPB to act as a final recourse when all other efforts by consumers to address fraud have failed.

Thank you again for your interest in and commitment to helping consumers who have been impacted by fraud and scams, and for the opportunity to answer your question.

Sincerely,



Carla Sanchez-Adams
 Senior Attorney
 National Consumer Law Center, on behalf
 of its low-income clients

Written Answers to Questions for the Record
 From Kate Griffin, Aspen Institute Financial Security Program
 For U.S. House of Representatives, Committee on Financial Services
 Sub-committee on Oversight and Investigations
 Hearing titled: "Fraud in Focus: Exposing Financial Threats to American Families"

September 18, 2025

Question from Representative Andrew Garbarino:

- **During the hearing, you raised the risk of crypto ATMs placed in nursing homes and retirement homes.**
 - **Can you provide the Committee with any data on how many crypto ATMs you discussed are in nursing homes and retirement communities?**
 - **Do you also have any data on where those crypto ATMs are located and the company that owns them?**

Thank you for this question and your concern for the risks posed to older Americans in particular, who have the highest dollar amount losses due to scams of any population.¹

As I shared in written testimony, over the last year the Aspen Institute Financial Security Program has convened the National Task Force on Fraud and Scam Prevention with over 80 institutions who play a role in preventing scams. Throughout the process of convening the Task Force, we received anecdotal reports concerning criminals who induce victims to use crypto ATMs to quickly convert cash into cryptocurrency. These funds are instantaneously transferred overseas to transnational criminal enterprises targeting Americans. These anecdotes included the placement of some ATMS in and near communities with a higher concentration of older Americans.

Data reported by the FBI indicates a potential correlation between crypto ATM use and financial crime. Last year, the FBI received approximately 11,000 complaints of cryptocurrency ATM fraud, totaling losses of \$246.7 million. Twenty-four percent of cryptocurrency ATM related complaints came from people aged 60 and over, accounting for 43% of the reported losses.² This age demographic's share of losses is notable when compared to the general population's

¹ Older adults reported losing more than \$1.9 billion to fraud in 2023. Because the vast majority of frauds are not reported, this figure represents only a fraction of the overall cost of fraud to older consumers in 2023, which the FTC estimates may be as high as \$61.5 billion. The FTC in 2023 showed that adults aged 60 and over were less likely to report losing money to fraud than adults aged 18-59. When they did report losing money, though, adults over 60 often reported losing substantially more than younger adults. See: "Protecting Older Consumers 2023-2024: A Report of the Federal Trade Commission." Federal Trade Commission, 2024. <https://www.ftc.gov/reports/protecting-older-consumers-2023-2024-report-federal-trade-commission>.

² "Internet Crime Report 2024." Internet Crime Complaint Center (IC3). April 24, 2025. www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report.

usage of cryptocurrency, which Pew reports as 8% of the population over age 50, compared with 29% of the population aged 18-29.³

Further information, such as the D.C. Attorney General's Office (OAG) case against Athena Bitcoin points to an association between crypto ATMs and scam activity. The OAG's investigation indicated that 93% of Athena ATM deposits were associated with scams, and the victim's median age was 71.⁴ FinCEN has also issued an alert urging financial institutions to be vigilant regarding the use of cryptocurrency ATMs, given the rise in associated scam activity.⁵

Additional study could investigate the locations of these machines. For example, a GIS mapping exercise in a Florida retirement community showed that crypto ATMs are located in close proximity to communities with a greater concentration of older residents, despite this population segment reporting lower rates of cryptocurrency use. (See Figure 1)

Our recent report, "United We Stand: A National Strategy to Prevent Scams" asks state governments to consider the merits of placing restrictions on, or outright banning, crypto ATMs. It further discusses possible measures such as daily caps on the use of crypto ATMs.⁶ To date, at least 11 states have passed laws or regulations concerning these machines, many as a result of the rise in scam activity associated with them.⁷

³ "Majority of Americans aren't confident in the safety and reliability of cryptocurrency." Michelle Faverio, Wyatt Dawson, and Olivia Sidoti. Pew Research Center. October 24, 2024. <https://www.pewresearch.org/short-reads/2024/10/24/majority-of-americans-arent-confident-in-the-safety-and-reliability-of-cryptocurrency/>

⁴ "Attorney General Schwalb Sue Crypto ATM Operator for Financially Exploiting District Residents." Press Release dated September 8, 2025. <https://oag.dc.gov/release/attorney-general-schwalb-sues-crypto-atm-operator#:~:text=illegally%20profiting%20from%20hidden%20fees,sufficiently%20heeding%20onscreen%20BTM%20warnings.>

⁵ "FinCEN Notice on the Use of Convertible Virtual Currency Kiosks for Scam Payments and Other Illicit Activity" FinCEN Notice dated August 4, 2025. <https://www.fincen.gov/system/files/2025-08/FinCEN-Notice-CVCKIOSK.pdf>

⁶ The National Task Force on Fraud and Scam Prevention, "United We Stand: A National Strategy to Prevent Scams," The Aspen Institute Financial Security Program, October 1, 2025. <https://fraudtaskforce.aspeninstitute.org/nationalstrategy>.

⁷ Kevin, Hardy. "Citing potential for fraud, blue and red states pass new crypto ATM laws," Stateline, July 28, 2025. <https://stateline.org/2025/07/28/citing-potential-for-fraud-blue-and-red-states-pass-new-crypto-atm-laws/>.

Figure 1: The Villages, FL