America's Credit Unions

Testimony of

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

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

Before the
Subcommittee on Financial Institutions
House Committee on Financial Services

March 5, 2026

Introduction

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

About Park Community Credit Union

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

Background on Credit Unions

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

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

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

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

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

The Challenge of Preventing Fraud

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

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

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

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

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

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

Types of Scams Impacting Credit Union Members

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

Check Fraud

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

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

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

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

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

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

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

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

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

Legislative Actions that Would Help Combat Growing Fraud Losses

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Legislation Noticed for this Hearing

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

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

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

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

Conclusion

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

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

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

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

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