Testimony of

Paul Benda

On Behalf of the

American Bankers Association

Before the

Special Committee on Aging

Of the

United States Senate

July 29, 2026

American Bankers Association®

Introduction

Chairman Scott, Ranking Member Gillibrand, and members of the Committee, thank you for the opportunity to testify for today's hearing entitled: "The AI Deception Machine: Deepfakes, Chatbots, and the New Frontier of Senior Fraud." My name is Paul Benda, and I serve as Executive Vice President for Risk, Fraud and Cybersecurity at the American Bankers Association. ABA is the voice of the nation's banking industry, which is composed of small, regional and large banks that together employ more than two million people, safeguard trillions of dollars in deposits, and extend credit in communities across the country.

Banks play a unique and essential role in supporting the financial health of older Americans. As trusted institutions deeply rooted in their communities, banks are often the first, and most consistent, financial touchpoint for seniors and their families. Every day, bank employees help older customers manage retirement income, protect their savings, recognize and avoid scams, and adapt to an increasingly digital financial system. These relationships position banks not only as providers of financial services, but also as front-line educators and protectors of financial security.

Banks have long used advanced analytics and artificial intelligence to identify suspicious transactions, protect customer accounts, and respond to cyber threats. Generative AI is strengthening those defensive tools. At the same time, criminals are using the same technology to make familiar scams more convincing, more personalized, cheaper to launch, and easier to scale.

The central point of my testimony is straightforward: generative AI is not replacing traditional scams. It is industrializing them. A criminal can now create a convincing voice, video, photograph, text message, advertisement, or online persona with little technical skill and at very low cost. AI allows fraudsters to imitate a friend, family member, bank employee, government official, physician, pastor, financial adviser, or virtually anyone else whose identity may inspire trust.

Older Americans face especially serious consequences from these scams. A loss may represent retirement savings that cannot be replaced, proceeds from a home sale, or money set aside for medical and long-term care needs. The financial damage can be compounded by shame, isolation, fear of losing independence, and reluctance to report the crime. We should be careful not to describe older Americans as inherently unsophisticated. These crimes succeed because professional criminals deliberately exploit trust, fear, urgency, family relationships, and authority. Generative AI makes those tactics substantially more credible.

My testimony focuses on four issues. First, I will describe how generative AI is changing the nature of scams. Second, I will explain why those changes are particularly significant for older Americans. Third, I will discuss what banks and ABA are doing to protect customers. Finally, I will offer practical steps for consumers and targeted policy recommendations for Congress and federal agencies.

Fraud Has Become an International Criminal Industrial Complex

Today's scams are often not isolated crimes committed by a lone opportunist. They are carried out by sophisticated domestic and transnational criminal networks that use stolen personal information, fake identities, money mules, fraudulent advertisements, spoofed calls and texts, fake websites, encrypted communications, and rapid payment channels. The infrastructure that

supports these crimes already exists, and generative AI is now being layered onto that infrastructure, making it even more effective.

AI can help criminals identify likely victims, collect personal information from public sources and data breaches, create customized scripts, translate communications into multiple languages, and sustain conversations with many victims at once. It can generate polished messages without the grammatical errors or awkward phrasing that once served as warning signs of a scam. It can also create synthetic identity documents and automate efforts to open accounts or take over existing accounts.

A recently published joint report by the ABA, Better Identity Coalition, and the Financial Services Sector Coordinating Council (FSSCC), *Mitigating AI-Powered Attacks Against Identity and Authentication*[1], identifies three broad AI-enabled attack vectors: deepfake-driven social engineering and impersonation, synthetic identity creation, and the use of AI agents as attack surrogates capable of automating account takeover and fraud activity. These threats affect both consumers and financial institutions, but for many older Americans the most immediate danger is the use of AI to make social engineering and impersonation scams more convincing, personalized, and difficult to detect.

How Generative AI Is Changing Scams Against Older Americans

The fundamental danger is that seeing or hearing someone can no longer be treated as proof of identity. A voice message may sound like a loved one. A video may appear to show a government official. A caller ID display may show the correct name and phone number of a bank. A social media account may use a familiar photograph and a convincing history of posts. Any of these signs of authenticity can be fabricated or manipulated.

Consumers have traditionally been advised to look for poor grammar, unnatural speech, obvious image defects, or inconsistent stories. Those remain useful clues, but they are becoming less reliable. A scam does not need to be technically perfect. It only needs to be credible enough, particularly when combined with urgency, secrecy, stolen personal information, and emotional manipulation.

A criminal can use information from social media, public records, obituaries, data brokers, breached accounts, and prior scam reports to tailor an approach. The scammer may know the names of family members, details from a recent trip, a medical condition, the victim's bank, or the identity of a trusted professional. That information can be woven into an AI-generated message or conversation, turning a generic scam into a seemingly personal emergency.

Generative AI enables a single criminal organization to maintain many apparent relationships at the same time. It can produce messages around the clock, adapt responses based on what a victim says, and translate content rapidly. This capability is especially dangerous in romance, investment, and recovery scams, where criminals may spend weeks or months building trust with their targets before requesting money.

A single fraud may begin with a social media advertisement, continue through text messages, move to a phone or video call, direct the victim to a fake website, and end with a bank transfer,

1 Financial Services Sector Coordinating Council, Mitigating AI-Powered Attacks Against Identity and Authentication (February 2026), https://fsscc.org/wp-content/uploads/2026/02/AI-IA-Workstream-Mitigations.pdf

cryptocurrency purchase, cash withdrawal, or courier pickup. Each channel can appear to confirm the others even when the entire experience is controlled by the same criminal group.

A Recent FBI Warning Shows the Threat in Practice

A July 20, 2026, public service announcement from the FBI's Internet Crime Complaint Center provides a timely example of how generative AI is being used to enhance and scale fraud schemes. The FBI warned that criminals are impersonating FBI and IC3 personnel to revictimize people who have already lost money. These scams use fake social media profiles, spoofed government websites, and AI-generated videos that depict senior FBI personnel encouraging victims to submit information through a fraudulent IC3 website.[2]

The alert is particularly important because it incorporates many of the defining features of this emerging threat. Criminals target prior victims, impersonate trusted authorities, use AI-generated videos to create a false sense of legitimacy, distribute content through social media, and direct victims to websites designed to collect personal and financial information. The promise of recovering stolen funds is itself a scam designed to steal even more money.

The FBI also warns that scammers may use AI-generated video during real-time chats to impersonate executives, law enforcement officials, or other authority figures. This illustrates why consumers cannot rely solely on the apparent realism of a video or voice. The correct response is independent verification through a trusted channel.

Scam Scenarios Particularly Relevant to Older Americans

Grandchild and family-emergency scams - A victim receives a call that sounds like a child, grandchild, or other relative in distress. The caller claims to have been arrested, injured, kidnapped, or hospitalized. A second person may pose as a lawyer, police officer, doctor, or court official. The victim is instructed to send money immediately and not contact other family members. Voice cloning can remove one of the most important reasons a victim might otherwise question the call.

Government and law enforcement impersonation - A criminal may claim to represent the FBI, Social Security Administration, IRS, Medicare, a local sheriff, or another agency. The victim may be told that benefits will be suspended, that an arrest is imminent, that an identity has been compromised, or that money must be transferred for safekeeping. The same tactic may be used in recovery scams, where the criminal falsely promises to recover an earlier loss in exchange for a fee or additional payment.

Bank-impersonation scams - A victim receives a text or call that appears to come from the bank's fraud department. The caller may know partial account information, refer to a supposed transaction, or cause the bank's actual number to appear on caller ID. The criminal may ask the victim to disclose an authentication code, approve a login, install remote-access software, or move funds to a supposed "safe account."

The FCC reinforced this warning in a July 21, 2026, consumer alert[3], noting that bank-impersonation scams account for the highest losses of any impersonation scam category

2 Federal Bureau of Investigation, Internet Crime Complaint Center, "FBI Warns of Scammers Impersonating the IC3," Alert No. I-072026-PSA (July 20, 2026), https://www.ic3.gov/PSA/2026/PSA260720.

3 Federal Communications Commission, FCC Consumer Alert: Bank Impersonation Scams (July 21, 2026).

and that victims may lose everything in their accounts. The FCC emphasized a simple rule: banks will never call or text consumers and ask them to move money to protect it.

A recent bank survey illustrates the scale of the problem. Among 14 surveyed large banks, the average number of identified bank-impersonation scams increased 150 percent from 2024 to 2025, reaching an average of 26,196 scams per bank. Telecom-originated scams increased 124 percent, while scams originating on social media more than doubled. The survey is not a census of the entire banking industry, but it provides strong directional evidence from institutions representing a significant share of industry assets.[4]

The same survey found that social media companies took nearly two weeks on average to remove bank-impersonation content and did not respond to more than 20 percent of takedown requests. Two surveyed banks reported that 40 percent of calls appearing to originate from bank-owned numbers had been spoofed. These results underscore that banks cannot stop impersonation scams alone. The deception often reaches the consumer through a telecom network, social media platform, advertising system, or messaging service before a bank sees any transaction.[5]

Romance and investment scams - AI-generated photographs, voice messages, video chats, and chatbots can help criminals build and sustain false relationships over long periods of time. A single criminal organization may manage many such relationships simultaneously. The relationship may eventually be used to persuade a victim to invest in a fraudulent scheme, send money in response to a manufactured emergency, receive and transfer funds, or participate in another form of financial exploitation. The emotional bond can make intervention extraordinarily difficult, even when family members or bank employees identify clear warning signs.

Technical-support and account-security scams - A criminal may impersonate a technology company, bank security specialist, or government cybersecurity official and claim that the victim's device or account has been compromised. The victim may be directed to install remote-access software, share a screen, reveal an authentication code, or transfer funds. AI-generated websites, instructions, and voices can make the approach look professional and legitimate.

Recovery and repeat-victimization scams - Prior victims are often targeted again by people claiming to be lawyers, investigators, banks, cybersecurity firms, or recovery services. The victim is promised that stolen funds have been located but must first pay a fee, tax, or processing charge. The recent FBI alert specifically warns about this form of "double-dip" scam. It is especially harmful because a prior victim may be emotionally vulnerable and desperate to recover retirement savings.

Why the Consequences for Older Americans Can Be Especially Severe

The financial impact of a scam can be devastating at any age, but older victims may have less time and fewer employment opportunities to rebuild savings. Losses may involve retirement assets, home equity, emergency funds, or money needed for health and long-term care.

4 Tara Payne, Drew Ruben & Madison Stulga, Bank Policy Institute, "Hijacking Trust: How Scammers Exploit the Banking System's Most Valuable Asset" (July 20, 2026), https://bpi.com/impersonation/. The survey covered 14 BPI member banks ranging from approximately $100 billion to more than $1 trillion in assets.

5 Id.

Victims may also hesitate to report. Some fear embarrassment or worry that family members will question their ability to manage their own finances. Others remain under the criminal's influence and believe that one more payment will resolve the emergency or recover prior losses. In romance scams, the victim may remain emotionally attached to the person they believe is real.

These dynamics make scam intervention different from ordinary transaction monitoring. Bank employees sometimes encounter customers who have been coached to lie about the purpose of a transaction, conceal communications, or distrust the very bank employee trying to protect them. Effective intervention therefore requires empathy, training, and an understanding of the psychological manipulation used by professional criminals.

How Banks Are Protecting Customers

Banks employ a host of tools to detect and deter fraud, including AI, machine learning, and other advanced analytics to identify unusual transactions, new or suspicious payees, account takeover, abnormal device activity, behavioral anomalies, manipulated documents, and high-risk payment patterns. These systems can surface transactions for additional review or prompt the bank to contact the customer before a transaction is completed.

While criminals use AI to make deception more effective, banks employ AI to detect anomalies and protect customers. The goal should not be to restrict beneficial defensive uses. It should be to strengthen safeguards, improve information sharing, and reduce criminals' ability to exploit communications and identity systems.

Banks increasingly employ layered defenses that combine identity validation, device and behavioral signals, document analysis, liveness and injection-attack detection, out-of-band verification, additional confirmation for high-risk activity, and human review. There is no single "deepfake detector" that can solve the problem. Effective defense depends on multiple independent signals and risk-based controls.

Technology alone, however, cannot identify every scam. Banks also rely on human judgment because no model, algorithm, or automated system can reliably detect every form of deception. Front-line bank employees are trained to recognize sudden payments to new recipients, unusual withdrawals, customers acting under extreme urgency, demands for secrecy, customers being coached over the telephone, and requests involving "safe accounts," cryptocurrency, gift cards, cash couriers, or other unusual payment methods.

ABA is expanding training that helps bankers recognize deepfakes and AI-enabled threats, support victims of financial crime, and intervene when a customer appears to be under a scammer's influence. That includes ABA's Spot the Scammer training and work focused on "breaking the scam spell," which recognizes that the challenge is not merely identifying an unusual transaction but helping a victim step outside the criminal's narrative.[6]

Fraud alerts and direct bank-customer communications are among the most effective tools available. A February 2026 Morning Consult poll commissioned by ABA found that nearly nine in ten bank customers said their bank takes proactive steps to protect them from fraud and scams.

6 American Bankers Association, "Spot the Scammer: How to Detect Scams, Deepfakes, and AI Threats," https://www.aba.com/training-events/online-training/spot-the-scammer.

Three in five consumers had received a fraud alert regarding potentially suspicious account activity, and 96 percent of those recipients found the alerts valuable.[7]

The same poll found that 72 percent of consumers believe banks do more than other industries to protect them from fraud and scams. By a margin of nearly five to one, consumers trusted banks more than other industries and the government to protect them from fraud. These findings are important because proposed legislation and the regulatory environment should support, rather than inadvertently impede, timely fraud alerts and other protective communications.[8]

Consumer education is an equally important component of fraud prevention. The ABA Foundation's Safe Banking for Seniors program provides banks with free, turnkey materials to educate older Americans, caregivers, and families about scams, identity theft, financial caregiving, and financial exploitation. More than 2,550 banks have participated in the program since it was launched in 2016.

ABA and the FBI have also developed consumer materials specifically addressing deepfake scams, and ABA maintains guidance explaining how deepfake media can be used in impersonation, investment, romance, employment, and other fraud schemes. ABA's #BanksNeverAskThat campaign teaches consumers to recognize common impersonation tactics, while the current "Snap Out of It!" theme focuses on interrupting the urgency and psychological manipulation used by scammers.[9]

ABA and the banking industry are working to improve the speed of bank-to-bank communications, standardize documentation used to request holds or returns of fraudulent funds, expand the ABA Fraud Contact Directory, and develop mechanisms for sharing fraud indicators. ABA is also working with law enforcement and other partners to improve recovery of funds, including funds moved through cryptocurrency.

These efforts are critical because modern fraud schemes span multiple institutions and industries. One bank may see the victim's outgoing payment, another may hold the receiving account, a telecom provider may carry the spoofed call, and a platform may host the fraudulent advertisement. No participant has the complete picture. Faster, privacy-protective sharing of fraud signals can allow earlier intervention and improve the chance of recovery.

What Older Americans and Their Families Can Do

Consumer guidance should be memorable, focused on the mechanics of impersonation, and avoid requiring people to become deepfake experts. The goal is to change the decision process so that a convincing voice or video cannot by itself trigger a payment. ABA recommends that seniors and their families take the following steps to guard against fraud:

> **Pause -** Do not act immediately, no matter how urgent or frightening the communication appears. Time is one of the most effective defenses against an AI-enabled scam because pausing interrupts the criminal's script and creates an opportunity to verify the story.

7 Morning Consult National Tracking Poll commissioned by the American Bankers Association, conducted Feb. 21-25, 2026, among 4,456 U.S. adults; margin of error +/- 1 percentage point.

8 Id.

9 American Bankers Association, "Deepfake Media Scams," https://www.aba.com/news-research/analysis-guides/deepfake-media-scams; American Bankers Association, "ABA Foundation and FBI Release New Infographic to Help Americans Spot and Avoid Deepfake Scams," https://www.aba.com/about-us/press-room/press-releases/ABA-Foundation-and-FBI-Joint-Infographic-on-Deepfake-Scams.

Verify through a separate channel - Hang up and contact the person or organization using a telephone number or method already known to be legitimate. Do not use a callback number, link, or website supplied by the caller or message. Call another family member before sending money. Contact the bank using the number printed on the card or statement.

Use a family password - Families should agree in advance on a private word or phrase that can be used to verify a genuine emergency. The phrase should not be posted online or easily guessed. A family can also establish a personal question whose answer is not available through social media or public records.

Remember: "If it's a secret, it's a scam" - A demand to act now, stay on the line, or keep the matter secret is a powerful warning sign. Criminals use secrecy to prevent victims from contacting family, banks, or law enforcement. A legitimate bank, government agency, police department, or family member should not object to independent verification.

Do not trust the channel itself - Caller ID can be spoofed. Voices can be cloned. Photographs and videos can be fabricated. Social media accounts can be copied or compromised. Seeing a familiar face or hearing a familiar voice is no longer sufficient proof of identity.

Never move money to a "safe account" - A bank or government agency will not direct a consumer to transfer funds to another account for protection. Requests involving cryptocurrency, gift cards, cash couriers, or payments to newly created accounts deserve particular scrutiny.

Involve a trusted person and report quickly - Before making a large or unusual payment, speak with a trusted family member, friend, banker, caregiver, attorney, or financial adviser. If money has already been sent, contact the bank immediately. Rapid reporting may improve the chance of stopping or recovering funds. Victims should also report the incident to the FBI's Internet Crime Complaint Center. The Senate Special Committee on Aging operates a Fraud Hotline that can help older Americans and families understand how to report scams and protect themselves.[10]

Most importantly, victims should not be shamed. These schemes are designed by professional criminals using sophisticated technology and psychological manipulation. Reporting quickly helps the victim and may help prevent others from being harmed.

Banks and Consumers Cannot Solve This Alone

By the time a bank sees a transaction, a criminal may have communicated with the victim for days or months. The deception may have been enabled by a spoofed call, fraudulent text, paid advertisement, social media account, messaging application, fake website, or cryptocurrency platform. Responsibility must extend to the sectors that enable criminals to reach and manipulate victims.

The Morning Consult poll referenced above found that three in four Americans had seen fraudulent or deceptive advertisements on social media. Seventy-eight percent supported federal

10 U.S. Senate Special Committee on Aging, Fraud Hotline, 1-855-303-9470, https://www.aging.senate.gov/fraud-hotline. The FBI also directs victims age 60 or older who need help filing an IC3 complaint to the Department of Justice Elder Justice Hotline at 1-833-FRAUD-11.

legislation requiring social media companies to do more to identify and remove fake accounts and fraudulent advertisements, and 77 percent supported regulatory action requiring telecommunications providers to do more to prevent spoofed caller IDs. Consumers clearly do not view scam prevention as solely a bank responsibility.[11]

Policy and Legislative Recommendations

We urge Congress and federal agencies to advance the following legislative and policy actions to strengthen the nation's ability to fight fraud and address the rapid rise in AI-enabled scams:

1. Establish a National Office for Scam and Fraud Prevention

ABA proposes legislation to establish a National Office for Scam and Fraud Prevention within the Executive Office of the President, led by a Senate-confirmed Director. The Office would develop and coordinate a National Scam and Fraud Prevention and Response Strategy, align federal agencies, promote real-time public-private information sharing, improve national fraud data, coordinate public education, support state and local capacity, strengthen international cooperation, and review relevant federal budgets.

This legislation is needed because fraud crosses agency, industry, jurisdictional, and national boundaries, while federal responsibility remains fragmented. No single official currently has the authority and accountability to coordinate prevention across the entire ecosystem. The proposed Office would shift the federal response from a collection of agency programs to a coordinated national strategy focused on prevention, disruption, victim support, and measurable outcomes.

2. Enact a Comprehensive Anti-Fraud Telecom Package

ABA has developed a five-part legislative package to address persistent weaknesses in the telecommunications system. The package is intended to prevent criminals from obtaining access to trusted communications infrastructure, improve the reliability of caller identity information, and enable faster intervention when an active campaign is underway.

Part I: Performance Bond

The first title would require providers filing in the Robocall Mitigation Database to post a performance bond of up to $100,000 unless the Federal Communications Commission (FCC) determines that a bond is unnecessary. Bad-actor shell providers can enter the market, facilitate large illegal calling campaigns, incur penalties, and disappear without meaningful assets. A bond would create a barrier to entry for fraudulent providers and a source of recovery when penalties are imposed.

Part II: Rapid Response to Active Threat Campaigns

The second title would establish an FCC rapid-response process for major, ongoing spoofing campaigns, with an objective of acting within 24 hours where practicable. It would authorize graduated actions, including formal traffic notifications, temporary cease-and-desist orders, and narrowly tailored blocking directives. It would also provide safe harbors for good-faith compliance and due-process protections for affected providers.

11 Morning Consult National Tracking Poll commissioned by the American Bankers Association, conducted Feb. 21-25, 2026, among 4,456 U.S. adults; margin of error +/- 1 percentage point.

This authority is needed because a high-volume campaign can cause substantial harm in hours or days, while traditional complaint and enforcement processes may take weeks or months. The government needs a mechanism capable of operating at the speed of scam.

Part III: Number Ownership Authentication and Attestation Integrity

The third title would create a Number Ownership Authentication Database and a neutral governance framework. Before assigning the highest level of STIR/SHAKEN attestation, an originating provider would be required to verify that the caller has the lawful right to use the number displayed to the recipient.

STIR/SHAKEN can help ensure that caller identity information is transmitted without alteration, but the framework cannot protect consumers if false information is improperly authenticated at the beginning of the call chain. ABA-supported analysis found substantial volumes of spoofed calls receiving A- or B-level attestation, demonstrating that the integrity of the system depends on meaningful verification by the originating provider.

Part IV: SIM Farm and SIM Box Prohibition

The fourth title would prohibit the manufacture, supply, possession, or operation of SIM farms and SIM boxes, subject to narrow lawful exceptions. These devices allow criminals to use a series of SIM cards to place large numbers of calls or messages that appear to originate from different numbers, making traceback and blocking substantially more difficult.

Part V: Database of Reported Scam Messages

The fifth title would create a secure database containing scam and spam messages reported by consumers through "Report Junk" and similar tools. Authorized businesses, banks, platforms, telecom providers, and anti-fraud organizations could use the data to identify active impersonation campaigns and warn consumers.

Today, messaging providers receive valuable reports about scam campaigns, but the businesses whose brands are being impersonated often cannot access that intelligence. A privacy-protective, near-real-time database would help transform isolated consumer reports into actionable warnings and mitigation.

3. Enact the SCAM Act

Social media and digital advertising platforms should verify advertisers, detect impersonation, provide free and accessible reporting channels, investigate reports rapidly, remove confirmed fraudulent content, and prevent repeat offenders from returning. Paid advertising deserves particular attention because platforms actively sell, target, curate, and profit from the content.

ABA strongly supports S. 3774, the Safeguarding Consumers from Advertising Misconduct Act, or SCAM Act. This bipartisan legislation would translate these expectations into enforceable obligations by requiring online platforms to verify advertisers' identities, maintain systems to detect impersonation, investigate reported fraudulent or deceptive advertisements within 72 hours, and notify the reporting individual, business, or government agency of the outcome within 24 hours after completing the investigation. By requiring meaningful prevention and timely action against fraudulent paid advertising, the SCAM Act would help stop scams before

criminals can establish trust and persuade victims to send money. Congress should enact it without delay.

4. Enact the National Payment Fraud Crime Control Act

ABA proposes the National Payment Fraud Crime Control Act, which would establish a Bureau of Justice Assistance grant program to help states create or strengthen Financial Crimes Intelligence Centers. These centers would coordinate the prevention, investigation, and prosecution of payment fraud, including both unauthorized transactions and payments victims are deceived into authorizing. Funding could support specialized investigators and analysts, training, technical assistance, centralized reporting, and information sharing among law enforcement, financial institutions, payment networks, and other partners.

The proposal builds on the Texas Financial Crimes Intelligence Center, a statewide fusion center staffed by experienced law enforcement officers and analysts that coordinates organized financial-crime investigations and works with federal, state, and local agencies and private-sector partners. Utah has also approved funding for a statewide Financial Crimes Intelligence Center within its Attorney General's Office. These models recognize that federal agencies cannot investigate every case and that state and local authorities need specialized capabilities to respond to the speed, volume, and complexity of modern fraud.

5. Require Strong Telecom Know-Your-Customer Controls and Enforcement

ABA commends the FCC and Chairman Carr for advancing proposals to require voice service providers to take specific actions to keep criminals off calling networks, including proposing stronger "know their customer" requirements for originating providers. In addition, we urge the FCC to require originating providers to collect and verify meaningful information about business callers before allowing them to use calling networks. Requirements should include legal identity, physical address, corporate formation and good-standing records, registration information, commercial presence, intended calling purpose, relevant ownership and compliance history, and evidence of financial responsibility.

ABA-supported analysis identified an originating provider that went from no calls to more than 136 million calls in a single month within two months of opening, with analysis indicating that most of the traffic was illegal. This example demonstrates why flexible and nonspecific expectations are inadequate. The FCC should establish clear standards, meaningful per-call penalties, allocate sufficient enforcement resources, and implement safeguards to prevent excluded bad actors from reentering the marketplace under new corporate identities

6. Modernize Identity and Authentication

Policymakers should support phishing-resistant authentication, digital mobile driver's licenses and other verifiable digital credentials, privacy-preserving government identity-validation services, clear regulatory treatment of modern credentials, and improved remote identity-proofing standards. These measures provide a long-term structural response to both deepfake fraud and synthetic identity creation.

7. Improve Information Sharing, Intervention, and Recovery

Congress should enact a new, fraud-specific information-sharing law rather than rely on further clarification of existing Bank Secrecy Act and anti-money-laundering authorities. FinCEN's

June 2026 Section 314(b) fact sheet[12] is helpful in confirming that participating financial institutions may share fraud-related information in real time, but Section 314(b) remains a voluntary AML framework built around suspected money laundering or terrorist activity, with eligibility, registration, use, and confidentiality requirements. It was not designed to support the automated, cross-sector, and cross-border exchange of actionable intelligence needed at the speed of scam.

The current legal and technical environment also lacks the common data standards, operating rules, and shared infrastructure necessary to exchange and act on fraud signals in real time. A new law must address not only what information may be shared, but also who will build, own, operate, secure, fund, and oversee the network through which that information moves.

Congress should establish an explicit safe harbor from federal and state liability for entities that, in good faith, send, receive, and act on fraud-risk information, including by delaying or restraining suspicious funds, while maintaining appropriate privacy, security, governance, and redress protections. The framework should support near-real-time sharing among financial institutions, telecommunications providers, digital platforms, payment systems, law enforcement, and trusted intermediaries; strengthen bank-to-bank freeze and recovery processes; and enable interoperability among domestic and international fraud-information networks. This approach is consistent with the recent Royal United Services Institute Future of Financial Intelligence Sharing report's call for more connected, cross-sector and cross-border platforms operating as a "network of networks," rather than isolated information-sharing arrangements[13].

8. Develop a Unified National Consumer Message

Government agencies, banks, telecom providers, technology platforms, law enforcement, community organizations, and senior-serving groups should reinforce the same simple actions: pause, verify independently, use a family password, refuse secrecy, and call the bank quickly.

Conclusion

Generative AI is making traditional impersonation scams faster, cheaper, more personalized, and more convincing. Older Americans may suffer especially severe and irreversible consequences. Banks are using advanced technology, employee intervention, education, information sharing, and recovery tools to protect customers, but banks cannot prevent fraud alone when the deception begins on a telecommunications network, social media platform, digital advertisement, messaging service, or fraudulent website.

Seniors should not be expected to distinguish, on their own and in real time, between a loved one and a synthetic voice, between a government official and an AI-generated video, or between their bank and a criminal using the bank's name and telephone number. The durable solution is to prevent criminals from exploiting the communications and technology systems that allow them to manufacture trust.

Congress can help by establishing accountable national leadership, strengthening telecommunications safeguards, improving information sharing and funds recovery, supporting modern identity systems, and ensuring that every sector involved in the scam lifecycle is responsible for protecting the public.

12 https://www.fincen.gov/system/files/shared/314bfactsheet.pdf
13 https://www.future-fis.com/fraudplatforms.html

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