UNITED STATES SENATE
SPECIAL COMMITTEE on AGING

ARTIFICIAL INTELLIGENCE & OLDER AMERICANS:

CONFRONTING NEW THREATS, UNLOCKING NEW OPPORTUNITIES

SEN. RICK SCOTT (R-FL)
CHAIRMAN

SEN. KIRSTEN GILLIBRAND (D-NY)
RANKING MEMBER

2026

TABLE OF CONTENTS

INTRODUCTION

AI'S IMPACT ON SENIORS

Artificial Intelligence (AI) is changing the way many Americans live and is being used noticeably in finance, national security, healthcare, criminal justice, transportation, and urban service delivery. AI is radically transforming our society, which is why policymakers must better understand its impact on all Americans, especially at-risk populations like seniors. As Congress works to address the questions presented by AI, it must ensure that the introduction and adoption of AI for seniors helps reduce costs, promotes their ability to age in place, and safeguards against fraud and scams. This report will analyze the risks stemming from AI-enabled fraud as well as the potential benefits of this emerging technology for older Americans.

HOW DOES ARTIFICIAL INTELLIGENCE WORK?

AI has been in development since the 1950s, steadily expanding in both capabilities and performance over the decades. Today, most of what is commonly referred to as AI is generative AI, which reached mainstream public awareness in the early 2020s with the release of consumer-facing tools capable of producing original text, images, and audio. Generative AI relies on sophisticated machine learning methods that examine extensive datasets, then produce original content reflecting the context, style, structure, and tone found in that source material. The primary advanced machine learning techniques for generative AI involve the use of layered deep neural networks as computational models, which work together to produce complex outputs.

FRAUD

While generative AI holds transformative implications for innovation and efficiency, it has also sparked an unprecedented surge in sophisticated scams that seniors are highly susceptible to. AI-generated scams, including deepfakes and voice cloning, are far more convincing and effective than traditional scams when used to target and victimize seniors. These scams often involve using AI to create realistic impressions of celebrities or a victim's loved ones. AI can also boost traditional scams through enhanced data collection or by generating high-quality responses for use by scammers.

The scope of victimization from AI-based fraud schemes in America today is staggering. Americans reported nearly $21 billion in cybercrime losses in 2025, with $893 million tied to AI-enabled scams across more than 22,000 complaints. Fraud targeting seniors has also escalated sharply across federal data sources. The FTC's Consumer Sentinel Network shows that total reported losses among adults 60 and older grew roughly fourfold between 2020 and 2024, climbing from approximately $600 million to $2.4 billion. Separately, the FBI's Internet Crime Complaint Center (IC3) reported that losses among this age group reached $7.7 billion in 2025, a nearly 60 percent increase over the $4.8 billion that IC3 attributed to this population in 2024.

DEEPFAKES

A deepfake is a video, photo, or audio recording that has been manipulated or generated by AI to seem authentic to its intended victim. AI can replace faces, manipulate facial expressions, synthesize faces, and synthesize speech to depict someone appearing to say or do something that they never said or did.

Deepfakes have historically been made using a type of AI called a Generative Adversarial Network (GAN), though some newer deepfake tools rely on other techniques such as diffusion models and transformer-based architectures. GANs work by setting two neural networks against each other, one that generates the fake image or video, the generator, and the other, the discriminator, which detects if images are real or fake. The generative network will make an image, and the discriminator network will then respond by saying whether it believes the image is real.

If the discriminator network does not believe the image is real, the generator network will remake another image taking input from the discriminator neural network. This process repeats until they reach an equilibrium in which the discriminator network can no longer distinguish real images from those generated by the generator network. These neural networks are developed by feeding hundreds or thousands of real images into the GAN, training them to identify and reconstruct patterns which are usually faces.

Deepfakes are used for a variety of different fraudulent and illicit purposes including investment fraud, impersonation, identity fraud, pornography, and general disinformation. Many deepfake frauds are used to target seniors. For example, 82-year-old Steve Beauchamp saw a video of what he thought was billionaire Elon Musk promoting a high-return investment opportunity. Mr. Beauchamp eagerly hopped on board. Within several weeks, Mr. Beauchamp lost more than $690,000 of his retirement savings to digital scammers, who used AI tools to create a convincing deepfake of Mr. Musk.

Another example is the case of 66-year-old Californian Abigail Ruvalcaba. After communicating online and through video messages, Ms. Ruvalcaba believed she had talked to and fallen in love with General Hospital actor Steve Burton. Unfortunately, she was actually talking with a scammer who had made deepfakes of Steve Burton. Ms. Ruvalcaba sent the scammer over $81,000 in cash. She also sold her condo far below market value and transferred most of the proceeds to the scammer, who ultimately cost her both her home and her savings.

VOICE CLONING

AI voice cloning is a technology that uses deep learning algorithms to create a highly accurate digital replica of a person's voice. By analyzing vocal traits like pitch, tone, and pacing from short audio samples, the AI can synthesize entirely new, natural-sounding speech that mimics the original speaker. It does this by combining several distinct types of neural networks together, in which each network's output becomes the next network's input, to make the final product.

Typically, a voice cloning AI system will work in the following manner: first, an AI speaker encoder network analyzes a voice sample, often sourced from videos posted on social media, to extract its unique characteristics such as tone, accent, and speech patterns. Then a text-to-speech synthesis network uses those characteristics to generate the content of the speech, and a vocoder network converts that output into a realistic audio waveform.

Each network passes its finished output forward as the input for the next, forming a pipeline of separate models rather than a single deep network.

Scammers will often use voice clones to impersonate a senior's loved ones, using a loved one's cloned voice to convince the senior that their loved one needs money for an emergency. One example is 82-year-old Floridian Sharon Brightwell, who received a call from a scammer posing as her daughter. The scammer played an AI voice clone of Ms. Brightwell's daughter that was crying and distraught, claiming she had been in a car accident and was in legal trouble. Believing it was her daughter, Ms. Brightwell complied when the scammer pleaded for immediate financial help to pay for bail and gave over $15,000 in cash to a courier who came to her home. Only after speaking to her daughter did Ms. Brightwell realize she had fallen victim to a scam and report it to the authorities.

ENHANCEMENTS TO ALREADY PRACTICED SCAMS

AI has sharpened traditional tools scammers have already been using. One example is phishing scams, where scammers send mass emails to impersonate trusted institutions, companies, or individuals to trick people into giving away sensitive information.

In the past, generic phishing emails were easier to spot because they often contained poor grammar, awkward phrasing, and generic messaging. The poor structure of most phishing emails meant they had a low success rate and required scammers to send out massive quantities of emails. AI has eliminated many of the common tells for phishing emails by enabling scammers to mass produce the more personalized and more successful spear-phishing emails at the click of a button, and over 82 percent of phishing emails are now created with the help of AI. Fully AI-automated spear-phishing emails have achieved a 54 percent click-through rate, the same rate as that of human expert-crafted spear-phishing emails and much higher than the 12 percent click-through rate of generic phishing emails. AI has also helped fraudsters to craft convincing scams up to 40 percent faster.

Additionally, AI has industrialized the fraud industry. Schemes that once required a highly trained coder can now be managed by technically unskilled criminals who purchase sophisticated AI scamming software "off the shelf." Scamming software sells on the dark web for as little as $20, allowing for a massive increase in the use of this nefarious software.

The industrialization of fraud and scams is facilitated through legitimate AI tools which have been copied into criminal equivalents with no ethical guardrails. One such example is FraudGPT, a black hat toolset capable of crafting phishing emails and scam pages that mimic real services, creating undetectable malware, facilitating credit card fraud, and facilitating digital impersonation. FraudGPT is a malicious large language model built on the same type of foundational AI architecture as ChatGPT. Unlike commercial systems, however, FraudGPT has all ethical safety guardrails deliberately removed, and is trained specifically on criminal use cases. The service has a subscription fee ranging from $200 per month to $1,700 per year, providing plug-and-play capabilities to less technically inclined threat actors.

Policing AI models such as FraudGPT is extremely difficult for several reasons including payment in cryptocurrency, use of The Onion Router (TOR) network, and bulletproof hosting. Cryptocurrency was developed to enable secure, decentralized digital transactions without relying on traditional financial intermediaries. While these features offer legitimate benefits of payment privacy and financial inclusion, they are also attractive to criminal actors. Although many cryptocurrency transactions are public on blockchain ledgers, these actors are difficult to trace without specialized blockchain analytics platforms. TOR is a network originally developed by the U.S. Naval Research Laboratory in the mid-1990s to protect sensitive government communications using multiple layers of encryption. Although TOR has been an important tool for democracy and human rights movements abroad, TOR's structure has permitted broad access to what we now refer to as the dark web. The dark web is primarily accessed through TOR and is the home of a large amount of illegal activity due to TOR's cover of anonymity. Lastly, bulletproof hosting refers to the practice of hosting providers intentionally and purposely not engaging in good faith with legal processes such as subpoenas or court orders. When authorities seek to shut down these hosting providers, the providers will employ a variety of techniques to remain operational. Those techniques include quickly reassigning their IP addresses, renting IP addresses from legitimate major cloud providers and routing criminal traffic through them, operating in countries with weak cybercrime enforcement, political unwillingness to cooperate with foreign law enforcement, or outright corruption.

PROTECTING SENIORS FROM AI-ENABLED FRAUD

The scale of fraud targeting American seniors documented throughout this report demands more than a policy response at the federal level. While law enforcement and legislative action are essential to addressing these scams, individual awareness and behavioral precautions remain effective tools available to seniors and their families today. This section outlines the key protective measures recommended by federal agencies and advocates, as well as the federal programs currently working to intervene on behalf of victims.

RECOGNIZING THE WARNING SIGNS

The most consistent finding across federal fraud data is that the scams causing the greatest harm to seniors share a common set of warning signs that, if recognized early, can prevent catastrophic losses. The FTC advises that any unsolicited contact by phone, text, email, or social media should be treated with immediate skepticism, regardless of how professional or urgent it appears. Scammers often rely on creating a false sense of urgency specifically to prevent the target from pausing to verify the situation with a trusted person.

The payment method a scammer requests is one of the clearest red flags available. Any request for payment via gift card, wire transfer, cryptocurrency, or cash is a near-universal indicator of fraud. Legitimate government agencies, technology companies, and financial institutions do not request payment through these channels under any circumstances. The FTC is explicit that it will never demand money, make threats, or instruct anyone to transfer funds. Seniors who receive such requests should hang up or disengage immediately and contact a trusted family member, financial institution, or law enforcement before taking any action.

For AI-specific threats like deepfakes and voice cloning, the FBI recommends establishing a family code word or verbal safe phrase that can be used to verify identity when a family member appears to be calling in distress. Because AI voice cloning can replicate a loved one's voice from as little as a few seconds of publicly available audio, the sound of a familiar voice is no longer sufficient verification on its own. A pre-arranged code word that only family members know provides a simple but highly effective layer of protection against grandparent scams and distress call fraud.

SLOWING DOWN BEFORE ACTING

The FBI's "Take a Beat" campaign is built around a single core principle: pausing before responding to any unsolicited communication involving money or personal information. The campaign emphasizes that criminals engineer situations to feel urgent and emotionally overwhelming because urgency bypasses the rational evaluation that would otherwise allow a target to recognize a scam. Seniors who feel pressured to act immediately should treat that pressure itself as a warning sign.

The FTC similarly recommends that before making any investment, sending any payment, or sharing any personal information with an unknown party, seniors first talk to someone they trust. This is especially important in the context of long-term investment fraud schemes, in which scammers cultivate a romantic or personal relationship with a victim over weeks or months before introducing a fraudulent investment opportunity, and then actively instruct victims not to tell family members about the relationship or investment, framing secrecy as a sign of intimacy or financial sophistication. This type of request for secrecy around a financial transaction should be treated as an immediate red flag.

PROTECTING ACCOUNTS AND PERSONAL INFORMATION

Several practical steps can significantly reduce a senior's exposure to fraud. The FTC recommends placing a free credit freeze with all three major credit bureaus, which prevents new accounts from being opened in a victim's name even if their Social Security number has been compromised. A credit freeze does not affect existing accounts or credit scores and can be lifted temporarily when needed.

Seniors should also review their financial accounts regularly for unauthorized transactions and consider setting up transaction alerts through their bank or brokerage. For those concerned about investment fraud, the Financial Industry Regulatory Authority's (FINRA's) BrokerCheck tool allows anyone to verify whether a financial advisor or investment platform is legitimately registered before sending funds. The proliferation of fake cryptocurrency investment platforms makes this verification especially important, as these platforms are specifically designed to appear identical to legitimate services.

REPORTING FRAUD

Underreporting is one of the most significant barriers to combating elder fraud. The FTC estimates the true losses experienced by older adults in 2024 may have been as high as $81.5 billion, compared to the $2.4 billion actually reported to federal agencies. In large part, that is because many victims do not report being scammed out of embarrassment, confusion, or a belief that nothing can be done. Reporting matters, even when recovery seems unlikely. The FBI's Internet Crime Complaint Center at IC3.gov aggregates reports to identify criminal patterns and connect individual cases to larger investigations, which can be used to disrupt scam networks before additional victims are harmed.

Operation Level Up, the FBI's proactive cryptocurrency fraud intervention program, launched in January 2024, demonstrates the direct value of reporting. By analyzing complaints filed with the Internet Crime Complaint Center, the FBI has identified victims actively in the middle of being scammed and intervened by contacting them directly before further losses occurred. As of the end of 2025, the program had notified more than 8,100 victims, with 77 percent of those contacted unaware they were being scammed. The estimated savings to victims exceeded $511 million. Some victims contacted by the FBI were preparing to liquidate retirement accounts or sell their homes to send additional funds to scammers at the time of intervention. The program also referred 80 victims to FBI victim specialists for suicide intervention, underscoring the devastating psychological toll scams inflicted beyond financial loss.

Seniors who believe they have been victimized can also contact the AARP Fraud Watch Network Helpline at 877-908-3360, which provides free support and guidance regardless of AARP membership status. The FTC's ReportFraud.ftc.gov accepts complaints from victims of all ages and feeds directly into the Consumer Sentinel database used by federal, state, and local law enforcement agencies nationwide.

AI BENEFITS

Although AI-facilitated frauds and scams demonstrate how generative AI can place older adults at risk, AI is a tool that can be used for good and bad. AI also has the potential to help our nation's aging population by improving the quality of care available to them and their ability to age in place.

EMERGING TECHNOLOGIES

AI LONELINESS CHATBOTS

One emerging use of AI that could be useful to seniors is AI chatbots designed to combat loneliness. A University of Michigan National Poll on Healthy Aging asked a national sample of U.S. adults ages 50–80 questions about loneliness. It found one in three adults (34 percent) reported feeling isolated from others in the past year. Research has linked social isolation and loneliness to higher risks for a variety of physical and mental conditions: high blood pressure, heart disease, obesity, a weakened immune system, anxiety, depression, cognitive decline, Alzheimer's disease, and even death.

In response, the New York State Office for the Aging (NYSOFA) has collaborated with several partners to bring new AI-driven technologies to combat loneliness. One such partner is Intuition Robotics, whose AI companion device, ElliQ, was deployed to over 800 older New Yorkers through a pilot collaboration with NYSOFA aimed at reducing isolation, encouraging engagement, promoting better health outcomes, and enabling residents to remain safely in their own homes.

Data from the NYSOFA pilot indicates that ElliQ users experienced a 95 percent drop in feelings of loneliness, along with substantial gains in overall well-being. Engagement has remained strong across the state, with participants interacting with their ElliQ devices more than 30 times per day, and over three-quarters of those interactions centered on supporting users' social, physical, or mental health.

Another example is NYSOFA's partnership with ONSCREEN, Inc. and its AI-powered virtual companion, Joy. The device connects directly to a senior's television to engage in daily conversations, facilitate mental engagement through games, trivia and art, offer medication reminders, and enable easy video calling. This type of companion AI chatbot offers a novel solution to senior loneliness and allows seniors to stay in place, which a vast majority of seniors prefer.

AI SCRIBES

Increasingly, health systems and providers are implementing an AI scribe system for clinical electronic health record (EHR) documentation to help save physicians time on administrative paperwork, increase productivity, and reduce burnout in the profession. This practice involves using an ambient AI scribe to record healthcare conversations with patients during appointments and transcribe them into clinical note drafts. The note drafts are reviewed and edited by the provider before being added to patients' medical records.

While this change in process may seem small, the impact is large given the scale of paperwork physicians typically face. The benefit of added efficiency is clear. Streamlining the note-taking process can help save physicians the time they would have spent writing notes themselves both during and after appointments, reduce their paperwork burden overall, and allow them to spend more quality time with patients. This is beneficial for older adults, particularly those with multiple chronic conditions or complex medication regimens, who may need more personalized attention and time to discuss their medical care or treatment protocol.

CLINICAL DECISION SUPPORT AND PREDICTIVE ANALYTICS AI

AI models are increasingly integrated into clinical decision making, leading to notable advancements across a range of medical fields. This progress is especially notable in sepsis detection, cancer diagnosis, and understanding multiple drug interactions, all of which have a significant impact on access to novel care for older adults. AI systems deployed for clinical decision support use deep learning techniques, in which a network built from many layers analyzes various forms of input data to produce an output aligned with its intended purpose.

Sepsis detection has seen substantial advancements through the use of narrow, task-specific deep learning models trained on structured EHR data. This progress on detection is particularly important for older adults who face an increased risk of sepsis due to the presence of comorbidities and other factors compromising their immunity. These narrow models use real time data from patients to predict sepsis before clinically observable manifestations appear. One such AI algorithm, the COMPOSER model, was used in the emergency departments at UC San Diego Health in order to quickly identify patients at risk for sepsis infection and resulted in a 17 percent reduction in mortality. Sepsis Watch, a deep learning model developed at Duke University in North Carolina, was studied using patient data from a community health system in Ohio to see if its performance held up outside its original setting. The study found that the model maintained strong predictive accuracy across all four sites tested, representing the first external validation of a sepsis deep learning model in a community-based health setting.

Cancer detection has also been radically transformed with the adoption of AI tools which assist doctors in complex image interpretation, quantitative tumor analysis, and clinical decision-making. As traditional radiology faces mounting pressure from rising cancer caseloads, radiologist fatigue, and interpretive inconsistency, AI models offer an incredible service through their abilities to automate many of these functions. Further, performance metrics in the reviewed studies approach or surpass those of experienced radiologists across lesion detection, segmentation accuracy, risk prediction, and molecular phenotype inference. These advancements in detection are particularly impactful for older adults, as advancing age is the most significant risk factor for developing cancer.

AI tools have also helped drive advancements in understanding drug-to-drug interactions, which remain a significant and intricate challenge in clinical pharmacology, as mixing drugs can have unintended and sometimes deadly consequences. Progress in this field is especially impactful for older adults, many of whom live with chronic conditions that require multiple medications to manage. Clinicians are increasingly using AI tools to evaluate molecular data and electronic health records to improve the precision and effectiveness of drug interaction prediction. The AI models have shown promise in identifying potentially inappropriate medications, medication reconciliation, and adherence monitoring. However, data regarding patient-level outcomes such as reductions in adverse drug reactions, hospitalizations, and mortality remains limited. This indicates the AI models are competent at identifying potential problems but less useful in changing behavior and require further development.

Despite these limitations, the trajectory of AI in drug interaction management is promising, and the clinical stakes for seniors make continued innovations in the field essential. Older adults face the greatest risk of pharmacological mismanagement, and the consequences of a missed interaction, including hospitalization, permanent injury, or death, are severe and often irreversible. As these tools mature and evidence accumulates, AI-assisted medication management has the potential to become a high-impact application of artificial intelligence for older adults. AI can potentially reduce preventable adverse drug reactions, lower hospitalization costs, and improve quality of life for the millions of seniors managing multiple chronic conditions.

AI AND AGING IN PLACE

The vast majority of American seniors want to remain in their own homes as they age. A 2025 Pew Research Center survey found that 93 percent of adults aged 65 and older currently live in their own home or apartment, and most say they would want to stay in their home and have someone care for them if they could no longer manage independently. That preference is also financially beneficial: in-home care for part-time assistance averages $21,600 annually, compared to $54,000 for assisted living and more than $116,000 for a private room in a nursing home. Despite the strong preference of older adults to age in place, significant safety challenges make doing so difficult. Each year, roughly 25 percent of Americans 65 and older experience a fall, amounting to about 36 million cases nationwide. These falls frequently cause fractures or head trauma, and the associated healthcare costs exceed $50 billion annually. Falls are one of the leading drivers of nursing home placement, making fall prevention a central challenge for aging in place.

AI-powered remote monitoring and fall detection systems address this challenge directly. These systems use data from wearable sensors, ambient sensors, and cameras to detect falls in real time and, increasingly, to identify fall risk before an incident occurs by tracking changes in gait, balance, and movement patterns over time. Beyond fall detection, AI-enabled remote monitoring platforms can track vital signs, medication adherence, sleep patterns, and activity levels continuously and can flag changes that may indicate a developing health problem and alert caregivers or clinicians before a condition requires emergency care or hospitalization. Patients using telehealth virtual medication reminders have already shown a 30 percent increase in medication compliance compared to those receiving in-person-only support, and telehealth is especially impactful for patients in rural or mobility-limited situations, reducing emergency room utilization and enabling earlier interventions.

While AI has only been partially integrated into these telehealth services, we can already see the blueprint for a large implementation of this emerging technology. A 2025 scoping review in *The Gerontologist* analyzed 32 empirical studies on AI applications for aging in place and identified meaningful potential across five domains: health and well-being monitoring, social inclusion, active aging, healthcare and end-of-life care, and community-level public health strategies. The review's findings support broader adoption of AI-enabled aging in place tools while noting that future research should validate these models across diverse populations and better account for the environmental and social factors that determine whether seniors can successfully age at home.

RISKS AND CONSIDERATIONS

The benefits of increasing AI implementation in the healthcare field are significant, but they do not come without risk, and a complete accounting of this technology's impact on seniors requires careful evaluation. Algorithmic bias is among the most serious concerns: AI models trained on datasets that underrepresent older adults may produce recommendations that are less accurate or inappropriate for the very population they are meant to serve. Current AI models are often developed using datasets that underrepresent older adults, particularly those who are racially and ethnically diverse, cognitively impaired, or from rural areas. This lack of diversity can introduce algorithmic bias that undermines the safety and efficacy of AI applications for these populations. For example, in the context of predicting risk for cardiovascular disease and diabetes, studies have found that algorithms consistently underperform for older adults, with researchers estimating that closing the age gap in model performance would require up to 192 percent more data from older patients. These are not abstract concerns: when AI clinical decision support tools perform less accurately for older patients, the consequences fall on the population that relies most heavily on those tools.

AI-driven claims review processes present a particular tension, as the same tools that could accelerate approvals can also be deployed to systematically deny care at scale in ways that are difficult for individual patients to identify or challenge. A 2023 investigation alleged that Cigna's PxDx algorithm was used to automatically review and deny more than 300,000 commercial insurance claims over a two-month period, with an average review time of just 1.2 seconds per claim. Multiple class action lawsuits followed, alleging Cigna used the tool to deny payment in batches of hundreds or thousands at a time without individualized medical necessity review, in violation of state law and the Employee Retirement Income Security Act (ERISA).

In March 2025, a federal court rejected Cigna's argument that having a medical director nominally sign off on the algorithm's output satisfied plan requirements for individualized review of each claim and allowed the lawsuit to proceed.

Cigna disputes that PxDx qualifies as AI or an algorithm at all, characterizing it instead as a standard verification tool applied only to a narrow set of low-cost, high-volume procedures. Similarly, use of AI to help make coverage decisions has increased in insurance plans covering low-income and older adults, and the underlying incentive structure raises cause for concern: automated systems that can review and deny claims in a fraction of a second create pressure to prioritize speed and volume over individualized clinical judgment, particularly when the resulting denials are unlikely to be appealed. That asymmetry, one side of the claims process gaining a powerful new tool while patients retain the same limited appeal capacity they have always had, raises the stakes considerably as similar technology spreads across the industry.

Given the serious potential risks involved with the deployment of AI in healthcare settings, any deployment of AI must be monitored to ensure it is being used in a legal and beneficial manner. That said, current evidence supports cautious optimism. The inefficiencies AI might correct are not minor inconveniences: they represent a massive administrative burden consuming hours of physicians' time annually that could otherwise go toward direct patient care, a physician burnout crisis that is driving experienced providers out of the profession, and a loneliness epidemic among older adults that carries measurable consequences for physical and mental health. The risks of AI in healthcare are real and must be managed through strong oversight, transparent outcome reporting, clear accountability standards, and careful engagement with patients, providers, and other stakeholders. But the risks of failing to adopt these tools, of leaving in place a system flawed in documented and costly ways, are just as real. It is the responsibility of both government and industry to ensure the role of AI in healthcare develops in a way that consistently puts the patient first.

POLICY RECOMMENDATIONS

The evidence presented in this report points to a set of actionable legislative and policy responses that address both the growing threat of AI-enabled fraud targeting older Americans and the significant opportunity AI presents to improve the quality and affordability of care for an aging population. The following recommendations reflect areas of documented bipartisan agreement and build directly on already-introduced legislation.

STOPPING FRAUD AGAINST SENIORS

ENACT THE NO FAKES ACT OF 2026

This legislation, introduced by Senators Coons, Blackburn, Tillis, and Klobuchar, would create a federal right prohibiting the creation or hosting of AI-generated replicas of a person's voice, image, or likeness without their consent, and would hold both producers and platforms that knowingly host such content liable. As the voice cloning cases documented in this report illustrate, scammers are already weaponizing this technology against seniors at scale, replicating a grandchild's voice from seconds of publicly available audio to manufacture fake distress calls demanding immediate cash transfers. No current federal law specifically prohibits the creation of an AI voice replica used for fraud, leaving prosecutors to rely on existing wire fraud statutes that were not designed for AI. The NO FAKES Act would close that gap by establishing consent as the governing standard, creating clear liability for those who produce or distribute unauthorized replicas, and providing victims an explicit federal right of action.

ENACT THE NATIONAL STRATEGY FOR COMBATING SCAMS ACT

This legislation, introduced by Chairman Rick Scott, Ranking Member Kirsten Gillibrand, Senator Kelly, and Senator Moody, would require the FBI to develop a unified national strategy incorporating input from victims, law enforcement, nonprofits, and the private sector. The Government Accountability Office has identified at least 13 federal agencies with roles in anti-scam enforcement, each operating under separate mandates with little coordination between them. A coordinated national strategy with clear ownership is a necessary foundation for the other enforcement efforts described below.

ENACT THE GUARD ACT

This legislation, introduced by Ranking Member Kirsten Gillibrand and Senator Britt, would expand existing federal grant programs to fund specialized law enforcement training on elder fraud and incorporate technology tools including blockchain tracing to follow stolen cryptocurrency. Cryptocurrency payment channels favored by foreign fraud networks are deliberately chosen for their resistance to tracing and recovery. The FBI's Operation Level Up has demonstrated that proactive, technology-assisted intervention in active fraud cases works. As of the end of 2025, the program had notified over 8,100 victims since its January 2024 launch, with 77 percent of those contacted unaware they were being scammed at the time and has prevented an estimated $511 million in losses. The GUARD Act would extend that kind of technical capacity to state and local law enforcement agencies that currently lack the tools to pursue these cases.

ENACT THE REPORTSCAMS.GOV ACT

This legislation, introduced by Chairman Rick Scott and Senator Hassan, would establish a centralized federal portal where consumers can report scams, access information about available assistance, and have their submissions automatically routed to the relevant federal and state law enforcement agencies. Victims would receive a tracking number and a list of the agencies that received their report, replacing the fragmented landscape in which potential victims must navigate the FTC, the FBI's Internet Crime Complaint Center, state agencies, and local law enforcement as separate reporting destinations for the same crime. The bill would also direct the development of a comprehensive Federal Scams Action Plan to improve coordination across agencies and strengthen enforcement. A single, trackable portal would reduce that friction for victims and generate a consolidated federal dataset enabling the kind of trend identification and rapid interagency coordination that AI-enabled fraud operations currently exploit by operating across jurisdictions. This legislation is supported by both the Chairman Rick Scott and the Ranking Member Kirsten Gillibrand.

REDUCE THE STIGMA OF REPORTING FRAUD AND USE EXISTING FRAUD EDUCATION RESOURCES

The FTC estimates that the true losses experienced by seniors in 2024 may have been as high as $81.5 billion compared to the $2.4 billion actually reported to federal agencies. The Aging Committee has made reducing reporting stigma a central theme of its fraud work, bringing awareness of the damage done by these scammers and showing how this issue affects everyday Americans, highlighting the need to report these crimes. Programs focused on protecting seniors from these types of digital scams should emphasize the ability and importance of reporting, showing seniors how and where to report these crimes.

ENACT THE TAX RELIEF FOR VICTIMS OF CRIMES, SCAMS, AND DISASTERS ACT

This legislation, introduced by Senators Baldwin, Moody, and Welch, would restore the tax deduction for personal casualty and theft losses, which allows victims of crimes and unexpected, uninsurable disasters to deduct their losses from their taxes. This ensures that victims of scams, robberies, natural disasters, and fires are not required to pay taxes on assets they have lost, helping to preserve their hard-earned savings and financial security. Until 2018, the federal tax code allowed victims of crimes and certain unexpected, uninsured disasters to deduct their losses through the “Casualty and Theft Loss Deduction.” Today, many scam victims and homeowners who suffer significant losses remain liable for tens or even hundreds of thousands of dollars in federal taxes unless their circumstances fall within a narrow set of exceptions. This legislation is supported by both the Chairman Rick Scott and the Ranking Member Kirsten Gillibrand.

USING AI TO IMPROVE SENIOR HEALTHCARE

ENACT THE IMPROVING SENIORS TIMELY ACCESS TO CARE ACT

This legislation, introduced by Senators Marshall and Warner, would codify electronic prior authorization standards for Medicare Advantage plans and require faster turnaround times on authorization requests. The bill addresses the administrative burden problem that many physicians face by streamlining and improving transparency of the prior authorization system. The current system inflicts massive costs on the healthcare system in administrative overhead, delays care for patients and contributes to physician burnout. Electronic standardization and mandatory timelines would work to address all three of these problems and represent a major step in modernizing this system. This legislation is supported by both the Chairman Rick Scott and the Ranking Member Kirsten Gillibrand.

ENACT THE AGING WITH ARTIFICIAL INTELLIGENCE ACT

This legislation, introduced by Senator Kelly and Chairman Rick Scott, would direct the Secretary of Health and Human Services, acting through the Director of the National Institute on Aging, to seek to enter into a contract with the National Academies of Sciences, Engineering, and Medicine to conduct a consensus study on the effects of artificial intelligence-enabled systems on older adults. This study would provide more information about the specific impacts of AI on older adults and allow for further insights into how this technology will impact our seniors.

SUPPORT REAUTHORIZATION OF THE OLDER AMERICANS ACT

This legislation, introduced by Senators Cassidy, Sanders, Chairman Rick Scott, and Ranking Member Kirsten Gillibrand, would reauthorize the Older Americans Act (OAA), which is the primary federal law supporting community-based services that allow older adults to remain in their homes. OAA programs, which served more than 10 million people in 2021, fund home-delivered meals, transportation, caregiver support, and a range of supportive services that are the non-technological complement to the AI-enabled monitoring and care tools that support aging in place. While AI can extend the period during which a senior can safely live independently, it cannot substitute for the meal delivery, in-home care, and community connection that OAA programs provide.

Reauthorizing and fully funding the OAA alongside investments in AI-enabled aging-in-place technology would ensure that both the technological and human infrastructure required for seniors to age safely at home is in place. As of July 2026, reauthorization of the Older Americans Act has passed the Senate with unanimous consent and is awaiting action in the House. This legislation is supported by both the Chairman Rick Scott and the Ranking Member Kirsten Gillibrand.

CONCLUSION

Harnessing the promise of artificial intelligence for older Americans while protecting them from its misuse is paramount. This report has examined two ways AI will impact American seniors' lives: the growing threat of AI-enabled fraud targeting them, and the significant opportunity AI presents to reduce their healthcare costs, ease administrative burdens, and extend quality care to an aging population.

In combating fraud, industrial-scale criminal networks pose a significant threat to our seniors, and we must identify them as the large-scale threat they are. The U.S. government must pursue public education efforts to reduce reporting stigma, raise awareness of the new wave of scamming methods AI enables, and teach seniors how to protect themselves from these new scams. Individual precautions matter, and in conjunction with actions to limit the reach and effectiveness of the industrial-scale criminal scamming networks, they will have a meaningful impact on protecting seniors.

In improving healthcare, AI's potential to reduce administrative burden, ease physician burnout, improve clinical outcomes, and extend independent living is already being realized. It is paramount that these capacities are allowed to continue to develop and are supported to allow us to bring the best, most efficient care to our seniors. The safe, responsible use of AI should be welcomed, and we should continue to research and evaluate the various beneficial impacts this emerging technology will have on the health of our seniors. Protecting seniors from AI-enabled fraud and expanding their access to AI-assisted care are not competing priorities, they are two sides of the same obligation. As AI continues to reshape every sector of American life, the U.S. Senate Special Committee on Aging is committed to ensuring that seniors share in its benefits and are shielded from its harms.

The following report was developed by the Majority and Minority staff of the United States Seate Special Committee on Aging at the direction of Chairman Rick Scott (R-FL) and Ranking Member Kristen Gillibrand (D-NY). This document has been developed for informational purposes. It does not represent findings or recommendations formally adopted by the committee.

ENDNOTES

INTRODUCTION

- https://www.brookings.edu/articles/how-artificial-intelligence-is-transforming-the-world/
- https://www.ibm.com/think/topics/artificial-intelligence
- https://www.poynter.org/fact-checking/2023/what-is-generative-ai-and-why-is-it-suddenly-everywhere-heres-how-tools-like-chatgpt-and-dall-e-work/
- https://www.congress.gov/crs-product/IG10077

FRAUD

- https://www.americanbar.org/groups/law_aging/publications/bifocal/vol45/vol45issue6/%20artificialintelligenceandfinancialscams/
- https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf
- https://www.ftc.gov/news-events/news/press-releases/2025/12/ftc-issues-annual-report-congress-agencys-actions-protect-older-adults
- https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf
- https://www.gao.gov/assets/gao-20-379sp.pdf
- https://onlinelibrary.wiley.com/doi/full/10.1155/int/9987535
- https://towardsdatascience.com/a-basic-intro-to-gans-generative-adversarial-networks-c62acbcefff3/
- https://www.ic3.gov/PSA/2024/PSA241203
- https://cybelangel.com/blog/deepfakes-stand-out/
- https://www.ncoa.org/article/understanding-deepfakes-what-older-adults-need-to-know
- https://www.nytimes.com/interactive/2024/08/14/technology/elon-musk-ai-deepfake-scam.html
- https://ktla.com/news/local-news/woman-loses-home-scammed-by-ai-deepfake-scammer-pretending-to-be-general-hospital-actor/
- https://www.resemble.ai/resources/understanding-ai-voice-cloning
- https://www.academia.edu/80827011/Voice_Cloning_a_Multi_Speaker_Text_to_Speech_Synthesis_Approach_based_on_Transfer_Learning preprint version available at https://arxiv.org/pdf/2102.05630
- https://www.cnn.com/2026/05/29/tech/ai-voice-cloning-scams-protect-yourself
- https://www.academia.edu/80827011/Voice_Cloning_a_Multi_Speaker_Text_to_Speech_Synthesis_Approach_based_on_Transfer_Learning preprint version available at https://arxiv.org/pdf/2102.05630
- https://www.academia.edu/80827011/Voice_Cloning_a_Multi_Speaker_Text_to_Speech_Synthesis_Approach_based_on_Transfer_Learning preprint version available at https://arxiv.org/pdf/2102.05630
- https://www.fox13news.com/news/dover-woman-loses-15k-after-scammers-used-artificial-intelligence-impersonate-daughter
- https://www.knowbe4.com/press/new-knowbe4-report-reveals-a-spike-in-ransomware-payloads-and-ai-powered-polymorphic-phishing-campaigns
- https://www.sciencedirect.com/science/article/pii/S0957417426004598
- https://doi.org/10.1016/j.eswa.2026.131546, preprint version available at https://arxiv.org/pdf/2412.00586
- https://sosafe-awareness.com/company/press/one-in-five-people-click-on-ai-generated-phishing-emails-sosafe-data-reveals/
- https://www.bitdefender.com/en-us/blog/hotforsecurity/ai-turbocharging-scams-interpol
- https://www.bloomberg.com/news/articles/2023-08-21/money-scams-deepfakes-ai-will-drive-10-trillion-in-financial-fraud-and-crime
- https://www.deloitte.com/us/en/insights/industry/financial-services/deepfake-banking-fraud-risk-on-the-rise.html
- https://www.infosecurityeurope.com/en-gb/blog/threat-vectors/generative-ai-dark-web-bots.html
- https://www.nytimes.com/2026/02/11/us/digital-currency-bitcoin.html
- https://www.aging.senate.gov/imo/media/doc/f57529d9-aa4d-34b8-2e16-1c4d42153913/Testimony_Burns%20Koven%2001.14.26.pdf
- https://www.torproject.org/about/history/
- https://sqmagazine.co.uk/dark-web-statistics/
- https://sqmagazine.co.uk/tor-statistics/

ENDNOTES

- https://www.trmlabs.com/resources/blog/us-australia-and-uk-sanction-russian-cybercrime-infrastructure-supporting-ransomware
- https://www.silentpush.com/blog/infrastructure-laundering/
- https://gbhackers.com/bulletproof-hosting/
- https://consumer.ftc.gov/articles/how-avoid-scam
- https://consumer.ftc.gov/articles/scammers-use-fake-emergencies-steal-your-money
- https://www.ftc.gov/news-events/news/press-releases/2025/12/ftc-issues-annual-report-congress-agencys-actions-protect-older-adults
- https://consumer.ftc.gov/consumer-alerts/2025/02/scammers-impersonate-ftc-officials-including-chairman-andrew-ferguson
- https://www.ftc.gov/news-events/news/press-releases/2025/12/ftc-issues-annual-report-congress-agencys-actions-protect-older-adults
- https://www.ic3.gov/PSA/2024/PSA241203
- https://www.fbi.gov/news/press-releases/fbi-announces-nationwide-take-a-beat-campaign-to-increase-awareness-of-frauds-and-scams
- https://www.fbi.gov/news/stories/operation-level-up-how-the-fbi-is-saving-victims-from-cryptocurrency-investment-fraud
- https://consumer.ftc.gov/articles/investment-scams
- https://www.ftc.gov/business-guidance/blog/2024/02/love-stinks-when-scammer-involved
- https://www.aging.senate.gov/imo/media/doc/age_of_fraud_scams_facing_our_nations_seniors.pdf, page 23-24
- https://consumer.ftc.gov/articles/credit-freezes-and-fraud-alerts
- https://brokercheck.finra.org
- https://www.cnbc.com/2025/12/13/financial-fraud-seniors-ftc.html
- https://www.ic3.gov/Home/About
- https://www.fbi.gov/how-we-can-help-you/victim-services/national-crimes-and-victim-resources/operation-level-up
- https://www.fbi.gov/how-we-can-help-you/victim-services/national-crimes-and-victim-resources/operation-level-up
- https://www.fbi.gov/how-we-can-help-you/victim-services/national-crimes-and-victim-resources/operation-level-up
- https://www.fbi.gov/how-we-can-help-you/victim-services/national-crimes-and-victim-resources/operation-level-up
- https://www.aarp.org/money/scams-fraud/fbi-report-fraud-2024/
- https://www.ftc.gov/enforcement/consumer-sentinel-network

AI BENEFITS

- https://ihpi.umich.edu/national-poll-healthy-aging/national-findings/trends-loneliness-among-older-adults-2018-2023
- https://www.nia.nih.gov/news/social-isolation-loneliness-older-people-pose-health-risks
- https://pubmed.ncbi.nlm.nih.gov/23749730/
- https://aging.ny.gov/news/nysofas-rollout-ai-companion-robot-elliq-shows-95-reduction-loneliness
- https://aging.ny.gov/news/nysofas-rollout-ai-companion-robot-elliq-shows-95-reduction-loneliness
- https://strohscheinlawgroup.com/ai-virtual-companion-pilot-is-supporting-seniors-in-2025/
- https://www.pewresearch.org/short-reads/2026/02/26/most-older-adults-who-live-at-home-want-to-age-in-place-but-they-arent-entirely-confident-theyll-get-to/
- https://westhealthmosaic.com/articles/the-invisible-assistant-how-ambient-intelligence-is-giving-doctors-their-most-precious-gifttime-with-patients
- https://ai.nejm.org/doi/full/10.1056/AIoa2400867
- https://pmc.ncbi.nlm.nih.gov/articles/PMC12698495/
- https://www.researchgate.net/publication/401800112_Artificial_intelligence_and_rule-based_decision_support_for_medication_optimization_in_older_adults_a_systematic_scoping_review_of_polypharmacy_management_tools_and_ethical_challenges
- https://www.ncbi.nlm.nih.gov/pmc/articles/PMC12562115/
- https://www.ncbi.nlm.nih.gov/pmc/articles/PMC11396550/
- https://www.ncbi.nlm.nih.gov/pmc/articles/PMC12380558/
- https://pmc.ncbi.nlm.nih.gov/articles/PMC11691596/

ENDNOTES

- https://health.ucsd.edu/news/press-releases/2024-01-23-study-ai-surveillance-tool-successfully-helps-to-predict-sepsis-saves-lives/
- https://www.nature.com/articles/s41746-025-01664-5
- https://pmc.ncbi.nlm.nih.gov/articles/PMC12698495/
- https://www.cancer.gov/about-cancer/causes-prevention/risk/age
- https://pmc.ncbi.nlm.nih.gov/articles/PMC3444856/
- https://www.researchgate.net/publication/401800112_Artificial_intelligence_and_rule-based_decision_support_for_medication_optimization_in_older_adults_a_systematic_scoping_review_of_polypharmacy_management_tools_and_ethical_challenges
- https://www.pewresearch.org/short-reads/2026/02/26/most-older-adults-who-live-at-home-want-to-age-in-place-but-they-arent-entirely-confident-theyll-get-to/
- https://point.com/blog/aging-in-place-2025
- https://academic.oup.com/innovateage/article/9/Supplement_1/S24/8263970
- https://www.mcknights.com/news/falls-raise-risk-of-nursing-facility-placement-among-older-adults-large-study-finds/
- https://academic.oup.com/innovateage/article/9/Supplement_1/S24/8263970
- https://nchstats.com/us-home-care-industry-stats/
- https://pubmed.ncbi.nlm.nih.gov/40243582/
- https://pmc.ncbi.nlm.nih.gov/articles/PMC12742854/
- https://www.futuremedicine.com/articles/ai-bias-a-problem-long-before-the-algorithm
- https://www.healthcaredive.com/news/cigna-lawsuit-algorithm-claims-denials-california/688857/
- https://www.nfp.com/insights/court-allows-lawsuit-over-ai-use-in-benefit-denials-to-proceed/
- https://www.fiercehealthcare.com/payers/cigna-hit-august-another-lawsuit-over-claims-denials-through-pxdx
- https://www.barchart.com/story/news/18788009/cigna-health-giant-accused-of-improperly-rejecting-thousands-of-patient-claims-using-an-algorithm
- https://pubmed.ncbi.nlm.nih.gov/41639200/
- https://www.ama-assn.org/practice-management/digital-health/five-physician-specialties-spend-most-time-ehr
- https://www.mgma.com/mgma-stat/physician-burnout-still-major-factor-even-as-unexpected-turnover-eases
- https://www.nia.nih.gov/news/social-isolation-loneliness-older-people-pose-health-risks
- https://pubmed.ncbi.nlm.nih.gov/23749730/

POLICY RECOMMENDATIONS

- https://www.congress.gov/bill/119th-congress/senate-bill/4591/text
- https://www.gao.gov/products/gao-25-107088
- https://www.congress.gov/bill/119th-congress/senate-bill/3355
- https://www.fbi.gov/how-we-can-help-you/victim-services/national-crimes-and-victim-resources/operation-level-up
- https://www.congress.gov/bill/119th-congress/senate-bill/2544/titles
- https://www.congress.gov/bill/119th-congress/senate-bill/4782/all-info
- https://www.ftc.gov/system/files/ftc_gov/pdf/P144400-OlderAdultsReportDec2025.pdf
- https://www.congress.gov/bill/119th-congress/senate-bill/1773
- https://www.congress.gov/bill/119th-congress/senate-bill/1816/text
- https://www.congress.gov/bill/119th-congress/senate-bill/4916
- https://www.congress.gov/crs-product/R43414
- https://www.congress.gov/bill/119th-congress/senate-bill/2120