S. HRG. 119–150

PROTECTING FLORIDA'S SENIORS: FIGHTING FRAUD AND FINANCIAL EXPLOITATION

HEARING

BEFORE THE

SPECIAL COMMITTEE ON AGING

UNITED STATES SENATE

ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

DORAL, FL

AUGUST 7, 2025

Serial No. 119–12

Printed for the use of the Special Committee on Aging

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
61–468 PDF WASHINGTON : 2025

SPECIAL COMMITTEE ON AGING

RICK SCOTT, Florida, *Chairman*

DAVE McCORMICK, Pennsylvania
JIM JUSTICE, West Virginia
TOMMY TUBERVILLE, Alabama
RON JOHNSON, Wisconsin
ASHLEY MOODY, Florida
JON HUSTED, Ohio

KIRSTEN E. GILLIBRAND, New York
ELIZABETH WARREN, Massachusetts
MARK KELLY, Arizona
RAPHAEL WARNOCK, Georgia
ANDY KIM, New Jersey
ANGELA ALSOBROOKS, Maryland

MCKINLEY LEWIS, *Majority Staff Director*
CLAIRE DESCAMPS, *Minority Staff Director*

C O N T E N T S

Page

Opening Statement of Senator Rick Scott, Chairman 1

PANEL OF WITNESSES

Hon. Rosie Cordero-Stutz, Sheriff, Miami-Dade County, Doral, Florida 4
Jeff Johnson, State Director, AARP Florida, St. Petersburg, Florida 10
Hon. Kathy Kraninger, President & CEO, Florida Bankers Association, Tallahassee, Florida 12
Brandy Bauer, Joint Center Director for the State Health Insurance Assistance Program (SHIP) Technical Assistance Center Senior Medicare Patrol (SMP) National Resource Center, Waterloo, Iowa 14

APPENDIX

PREPARED WITNESS STATEMENTS

Hon. Rosie Cordero-Stutz, Sheriff, Miami-Dade County, Doral, Florida 32
Jeff Johnson, State Director, AARP Florida, St. Petersburg, Florida 34
Hon. Kathy Kraninger, President & CEO, Florida Bankers Association, Tallahassee, Florida 41
Brandy Bauer, Joint Center Director for the State Health Insurance Assistance Program (SHIP) Technical Assistance Center Senior Medicare Patrol (SMP) National Resource Center, Waterloo, Iowa 45

PROTECTING FLORIDA'S SENIORS: FIGHTING FRAUD AND FINANCIAL EXPLOITATION

Thursday, August 7, 2025

U.S. SENATE
SPECIAL COMMITTEE ON AGING
Washington, DC.

The Committee met, pursuant to notice, at 10:00 a.m., in Doral, Florida, Hon. Rick Scott, Chairman of the Committee, presiding.

Present: Senator Scott

OPENING STATEMENT OF SENATOR RICK SCOTT, CHAIRMAN

Chairman SCOTT. The U.S. Senate Special Committee hearing on Aging will now come to order. Thank you all for being here today. It is wonderful to be back home in Florida as we continue doing the work of this Committee.

The way this Senate job works is you don't want to miss any votes, so we are up there 40 to 42 weeks a year, and so it is a little harder than my time as Governor to get around the state, but it is nice to be here.

I want to have a big thank-you to the Miami-Dade County Sheriff's Department and the sheriff for hosting us here today.

I would like to recognize there are a lot of local leaders here and a lot of friends that I have had the opportunity to create relationships with over the last 15 years since I started running for Governor who are joining us today for this very important discussion.

One of the biggest issues I hear about from Floridians and seniors around the country is the growing threat of scams, fraud, and financial exploitation. Whether it is a phone call from someone posing as a grandchild in trouble, a suspicious investment scheme delivered through the mail, or an email from a government imposter threatening jail time, these criminals are targeting our seniors with increasing sophistication, and I think it has impacted almost every family.

Our seniors are often especially vulnerable to this kind of fraud. Sadly, for many older Americans, falling victim to a scam doesn't just mean losing money, it can also mean losing peace of mind, trust in others, and confidence in themselves on navigating daily life.

As this Committee has heard many times before, this is a multi-billion-dollar-a-year problem. In 2024, Americans over 60 years of age lost a staggering $4.8 billion to scams, and that is scams that

were reported. Many seniors don't report being scammed out of fear, shame, or the simple belief that nothing can or will be done, which is too bad that people believe that way. Everybody I know in law enforcement around the country, they would like to help. Many also aren't sure where or how to go about reporting what happened.

Unfortunately, the status quo for too long in Washington has been to hold hearings, issue reports, and move on to the next issue without ever taking meaningful steps to fix the problem. We all know that is unacceptable, and we cannot let that happen here, especially when our parents, our grandparents, our neighbors, our friends are being actively targeted by criminals every day. Many seniors live on fixed incomes, and this kind of exploitation can be the difference between comfortable retirement filled with connection and security and financially struggling through their golden years with feelings of distrust and isolation.

That is why we are focused on combating fraud and scams at every level. We need to highlight and discuss how we can effectively empower seniors, families, and our communities to safeguard themselves and our aging friends and neighbors against these scam artists, and then we must act to fight back and protect seniors. Many of these actions are highlighted in our 2025 Fraud Report, which I think you can pick up right out as you walk in.

I am grateful to my colleagues on this Committee for working with me to put this report together. By the way, I have a great team led by McKinley on the Committee, and they do a great job trying to help seniors. The report, which is also available online at Aging.Senate.gov/scam, includes helpful information meant to prevent fraud and provide resources for our seniors to report scams when they happen.

It is time we have to stop playing defense and start going on the offense. We must support our law enforcement at every level, educate the public, and get innovative on how we protect vulnerable Americans. That is why we are right here in the great State of Florida for today's hearing. Our state is home to more than four million seniors. It is a hotspot for retirees and, unfortunately, scam activity. That is why I made it a priority to work with local, state, and federal law enforcement, community groups, and our state leaders to fight fraud head on.

We also need to take a hard look at where many of these scams are coming from, and this can't just be done locally. We have got to do this at the federal level also. Increasingly, we are seeing coordinated transnational fraud operations, especially from Communist China and other foreign adversaries, and let's not forget, they are adversaries. All right? Communist China is an adversary. If you buy something from Communist China, you are helping an adversary. They are talking to our seniors right here at home.

These aren't isolated incidents. They are large-scale operations run from overseas call centers, often with the knowledge or even the protection of regimes like the Chinese Communist Party. These groups use stolen data, AI technology, and cryptocurrency to exploit vulnerable Americans. This is more than just a consumer protection issue. It is a national security concern. We need to treat it

like one and hold these foreign actors accountable for enabling criminal activity that harms American seniors.

I have introduced the Stop Scammers Act. This bill will give the Treasury Department the authority to formally designate scam networks as foreign financial threat organizations and freeze their assets, cutoff their communication lines, and block their access to our financial system, and one thing we have got to do is we have got to make sure—and I have talked to Kash Patel about this and Pam Bondi—we have got to make sure our foreign resources, you know, are focused on the things that have to be done at the federal level and don't continue to focus on the things that the local sheriff's departments and police departments can do. If a foreign organization is preying on American seniors, they should be treated with the same seriousness and penalties as any other threat to our national security. That is exactly what the Stop Scammers Act allows us to do.

Today, we will hear from leaders who are combating this issue on the frontlines in our communities. We will hear how they are working to fight fraud and protect our seniors. Our goal today is simple: Educate the public on this important issue and start removing the stigma associated with reporting fraud and scams when they happen. There are a lot of people that are embarrassed, so they don't want to report it. They don't want to tell their families, and they clearly don't want to call law enforcement. We will hear from our community leaders on how to accomplish this, what proactive steps we can take to protect our vulnerable populations against scammers, and how we can empower seniors to recognize these threats.

Seniors deserve to feel safe when answering the phone, opening their email, and trusting the people around them. They also deserve to feel like they will be heard, that their concerns are valid when they report fraud to local authorities. Oftentimes, it is local law enforcement that is left to pick up the pieces by supporting victims, investigating these crimes, and trying to stop them from happening again.

This is one of the reasons I and Ranking Member Gillibrand joined with Senator Britt to introduce the GUARD Act. This bill supports law enforcement investigations into scams against retirees and expands the use of existing grants to go into fraud networks. The work our law enforcement plays in identifying and investigating scams against retirees is crucial to this fight.

Our first witness knows that reality all too well and has been a leader in showing how local agencies can fight back. Sheriff Rosie Cordero-Stutz is one of our state's finest law enforcement officials and brings decades of experience to her role protecting residents of Miami-Dade County. I am very appreciative of the sheriff. We got to know each other before she ran for sheriff. She is somebody that really cares about law enforcement. She has a law enforcement background. She cares about the law enforcement community and her community, and she is doing a great job.

Sheriff, we are grateful that you are here today. Thank you for your service, for being a champion for the safety and dignity of older Americans.

Please begin your testimony.

STATEMENT OF HON. ROSIE CORDERO-STUTZ, SHERIFF, MIAMI-DADE COUNTY, DORAL, FLORIDA

Ms. CORDERO-STUTZ. Good morning, Chairman, distinguished panelists, and everyone present. Welcome to the Miami-Dade Sheriff's Office. This is your home.

Thank you, Chairman Rick Scott, for your leadership and continued commitment to protecting America's seniors. It is an honor to stand beside you or sit beside you in this critical fight.

Florida is home to one of the largest senior populations in the country, and here in Miami-Dade County, we are proud of the enormous value of our older residents and what they bring with their families, our neighborhoods, and our history, but as Chairman Scott has long understood, our seniors also face growing threats from scams, abuse, and financial exploitation, and those threats are only becoming more sophisticated.

Since taking office in January, I made a promise to our residents to do everything in my power to protect our elderly population from harm. That is why I launched a set of online tools to make it easier for people to report fraud and abuse. I have said it before, and I will say it again. These deceptive schemes can cause lifechanging harm, but awareness and prevention can make all of the difference.

Chairman Scott's work on the U.S. Senate Special Committee on Aging is a beacon of leadership. His dedication through the TRACED Act, which is Telephone Robocall Abuse Criminal Enforcement and Deterrence, and pushing for the reauthorization of the Older Americans Act shows his deep understanding that protecting seniors is not just a policy priority, it is a moral responsibility.

Chairman Scott has reminded us that more than 10 million Americans benefited from the Older Americans Act program last year. That includes meal deliveries, transportation, and day services. Those programs provide much-needed support to the elderly. Through visitations, workers can detect signs of abuse or neglect.

At the Miami-Dade Sheriff's Office, our Cyber Crimes Bureau and Economic Crimes Section are working around the clock. From AI-generated scams to cryptocurrency theft and robocalls threatening arrest, these crimes are devastating. Retirement funds are wiped out, victims are saddled with debt, and many are left feeling embarrassed, isolated, and afraid.

Our Cyber Crimes Bureau is staffed with highly trained investigators who are leading the charge, working with cryptocurrency exchanges around the globe, including in countries where treaties fall short, to recover stolen funds. We have seen scammers use AI scripts to generate fake websites and realistic investment dashboards. They prey on our seniors through messaging apps, removing human interaction and making detection harder.

That is why timeliness matters. The faster the scams are reported, the better our chances are at stopping them before they vanish and reappear under a new name. We will continue to strengthen interagency collaboration. That means stronger ties with federal partners like the FBI, Homeland Security investigations, and the Department of Business and Professional Regulation.

We must not forget the growing threat of condo and HOA fraud occurring right here in our backyard, a quiet crisis disproportion-

ately affecting our elderly homeowners. One of my first actions as sheriff was to set up a hotline and an email address for people to call if they suspect public or HOA corruption.

Elderly residents are particularly vulnerable to fraud schemes involving unauthorized assessments, embezzlement, and falsified records. These crimes often go unreported or under-investigated due to the complexity of association governance and legal frameworks. We are working with state regulators to detect fraud in these associations and protect the rights of vulnerable residents.

Preventing fraud begins with education, as many homeowners are unaware of their rights. We have a public outreach initiative to empower residents and will continue to do so. To our residents, don't share Social Security numbers or banking information over the phone. Hang up on suspicious callers. The level of sophistication with regard to such scams is increasing. If you get a call from a relative or friend and they tell you to send them money immediately, verify it by calling them back on a trusted number. Never let urgency override common sense.

To our agency partners, let's keep pushing. Let's coordinate more, train more, and share more because in a perfect world, every senior in our community should live safe, supported, and scam-free.

Thank you, and thank you again, Chairman Scott, for standing with us on this mission.

Chairman SCOTT. Sheriff, would you like to say anything in Spanish, just a summary?

Ms. CORDERO-STUTZ. A summary.

Buenos días presidente, distinguidos panelistas y todos los presentes. Bienvenidos a la oficina de la Sheriff de Miami-Dade. Esta es su casa. Gracias, presidente Rick Scott, por su liderazgo y compromiso continuo para proteger a las personas mayores de Estados Unidos. Es un honor estar a su lado en esta lucha crítica.

Florida es el hogar de una de las poblaciones de personas mayores más grandes del país, y aquí en el Condado de Miami-Dade, estamos orgullosos del enorme valor que nuestros residentes mayores aportan a nuestras familias, nuestros vecindarios y nuestra historia. Pero como el presidente Scott ha entendido durante mucho tiempo, nuestros adultos mayores también enfrentan amenazas crecientes de estafas, abusos y explotaciθn financiera. Y esas amenazas solo se están volviendo más sofisticadas.

Desde que asumí el cargo en enero, hice una promesa a nuestros residentes: hacer todo lo que esté a mi alcance para proteger a nuestra población de ancianos de cualquier daño. Es por eso que lancé un conjunto de herramientas en línea para facilitar que las personas denuncien fraudes y abusos. Lo he dicho antes y lo diré de nuevo: estos esquemas engañosos pueden causar daños que cambian la vida. Pero la conciencia y la prevención pueden marcar la diferencia.

El trabajo del presidente Scott en el Comité Especial sobre el Envejecimiento del Senado de los Estados Unidos es un faro de liderazgo. Su dedicaciθn a través de la Ley TRACED (Teléfono, Robocall, Abuso, Ejecución Criminal y Disuasión) y su impulso para la reautorización de la Ley de Estadounidenses Mayores muestra su profundo conocimiento de que proteger a las personas mayores

no es solo una prioridad política, es una responsabilidad moral. El presidente Scott nos ha recordado que más de 10 millones de estadounidenses se beneficiaron del programa de la Ley de Estadounidenses Mayores el ano pasado. Eso incluye entrega de comidas, transporte y servicios diurnos. Esos programas brindan un apoyo muy necesario a los ancianos. A través de las visitas, los trabajadores pueden detectar signos de abuso o negligencia.

En la Oficina del Sheriff de Miami-Dade, nuestra Oficina de Delitos Cibernéticos y la Sección de Delitos Económicos estμn trabajando las 24 horas del día. Desde estafas generadas por IA hasta robo de criptomonedas y llamadas automáticas que amenazan con arresto, estos delitos son devastadores. Los fondos de jubilación son eliminados, las víctimas cargan con deudas y muchos se sienten avergonzados, aislados y asustados.

Nuestra Oficina de Delitos Cibernéticos cuenta con investigadores altamente capacitados que lideran la carga trabajando con intercambios de criptomonedas en todo el mundo, incluso en países donde los tratados son insuficientes, para recuperar fondos robados. Hemos visto a los estafadores usar scripts de IA para generar sitios web falsos y paneles de inversión realistas. Se aprovechan de nuestros adultos mayores a través de aplicaciones de mensajería, eliminando la interacción humana y dificultando la detección.

Por eso es importante la puntualidad. Cuanto más rápido se denuncien las estafas, mayores serán nuestras posibilidades de detenerlas antes de que desaparezcan y reaparezcan con un nuevo nombre.

Continuaremos fortaleciendo la colaboración interinstitucional. Eso significa lazos más fuertes con socios federales como el FBI, Investigaciones de Seguridad Nacional y el Departamento de Regulación Comercial y Profesional.

Y no debemos olvidar la creciente amenaza de fraude de condominios y asociaciones de propietarios que ocurre aquí mismo en nuestro patio trasero, una crisis silenciosa que afecta de manera desproporcionada a nuestros propietarios de viviendas mayores. Una de mis primeras acciones como alguacil fue establecer una línea directa y una dirección de correo electrónico para que las personas llamaran si sospechaban de corrupción pública o de la Asociación de Propietarios. Los residentes de edad avanzada son particularmente vulnerables a esquemas de fraude que involucran evaluaciones no autorizadas, malversación de fondos o registros falsificados. Estos delitos a menudo no se denuncian o no se investigan lo suficiente debido a la complejidad de la gobernanza y los marcos legales de las asociaciones.

Estamos trabajando con los reguladores estatales para detectar el fraude en estas asociaciones y proteger los derechos de los residentes vulnerables. La prevención del fraude comienza con la educación, ya que muchos propietarios desconocen sus derechos. Tenemos una iniciativa de divulgación pública para empoderar a los residentes y continuaremos haciéndolo.

A nuestros residentes: no compartan su número de Seguro Social o información bancaria por teléfono. Cuelgue las llamadas sospechosas. El nivel de sofisticación con respecto a tales estafas está aumentando. Si recibe una llamada de un familiar o amigo y

le dicen que le envíe dinero de inmediato, verifíquelo llamándolo a un número de confianza. Nunca dejes que la urgencia anule el sentido común.

A nuestras agencias y socios: sigamos presionando. Coordinemos más, capacitemos más y compartamos más. Porque en un mundo perfecto, todas las personas mayores de nuestra comunidad deben vivir seguras, apoyadas y libres de estafas.

Gracias y gracias de nuevo, presidente Scott, por apoyarnos en esta misión.

Chairman SCOTT. El Comité Especial sobre el Envejecimiento del Senado de EE. UU. ahora entrará en orden.

Gracias a todos por estar aquí hoy. Es maravilloso estar de vuelta en casa en Florida mientras seguimos haciendo el trabajo de este comité.

La forma en que funciona este trabajo en el Senado es que no queremos perder ninguna votación, y estamos en Washington de 40 a 42 semanas al año. Moverse por el estado es más difícil que en mi tiempo como Gobernador, pero es agradable estar aquí de nuevo.

Quiero agradecer enormemente al departamento de la Sheriff del Condado de Miami-Dade y a la Sheriff por recibirnos aquí hoy. Hay muchos líderes locales aquí y muchos amigos con los que he tenido la oportunidad de crear una relación durante losúltimos 15 años desde que comencé a postularme para Gobernador, y quienes se unen a nosotros hoy para una discusión muy importante.

Uno de los mayores problemas que escucho de los floridanos y las personas mayores de todo el país es la creciente amenaza de estafas, fraudes y explotación financiera.

Ya sea una llamada telefónica de alguien que se hace pasar por un nieto en problemas, un sospechoso plan de inversión entregado por correo o un correo electrónico de un impostor del gobierno amenazando con tiempo en la cárcel, estos criminales están apuntando a nuestros ancianos con cada vez más sofisticación. Y creo que ha impactado a casi todas las familias.

Nuestros adultos mayores a menudo son especialmente vulnerables a este tipo de fraude. Lamentablemente, para muchos Estadounidenses mayores, ser víctimas de una estafa no solo significa perder dinero; también puede significar perder la tranquilidad, la confianza en los demás y la confianza en sí mismos mientras navegan la vida diaria.

Como este comité ha escuchado muchas veces antes, este es un problema de miles de millones al año.

En 2024, los estadounidenses mayores de 60 años perdieron la asombrosa cantidad de $4.8 mil millones por estafas y eso es justo lo que se han reportado las estafas.

Muchas personas mayores no informan haber sido estafadas por miedo, vergüenza o la simple creencia de que nada se puede hacer ni se hará. Muchos tampoco están seguros de dónde o cómo hacer para denunciar qué pasó. Todos los que conozco en la aplicación de la ley en todo el país quieren ayudarlo.

Desafortunadamente, el statu quo durante demasiado tiempo en Washington ha sido celebrar audiencias, informes de problemas y pasar al siguiente problema sin tomar medidas significativas para solucionar el problema.

Todos sabemos que eso es inaceptable, y no podemos permitir que eso suceda aquí. Especialmente cuando nuestros padres, abuelos, vecinos y amigos están siendo atacados activamente por criminales todos los días.

Muchas personas mayores viven con ingresos fijos, y este tipo de explotación puede ser la diferencia entre una jubilaciθn cómoda llena de conexión y seguridad, y financieramente luchando durante sus años dorados con sentimientos de desconfianza y aislamiento.

Es por eso que nos enfocamos en combatir el fraude y las estafas en todos los niveles.

Necesitamos resaltar y discutir cómo podemos empoderar de manera efectiva a las personas mayores, las familias y nuestras comunidades para protegerse a sí mismos y a nuestros amigos y vecinos ancianos contra estos estafadores. Y luego debemos actuar para luchar y proteger a las personas mayores.

Muchas de estas acciones se destacan en nuestro Informe de fraude de 2025. Estoy agradecido con mis colegas de esta comisión por trabajar conmigo para elaborar este informe.

El informe, que está disponible en línea en Aging.Senate.Gov/Scam, incluye Información útil destinada a prevenir el fraude y proporcionar recursos para que nuestras personas mayores reporten las estafas cuando ocurren.

Es hora de que dejemos de jugar a la defensiva y comencemos a la ofensiva. Debemos apoyar a nuestros oficiales de la ley y el orden en todos los niveles, educar al público e innovar en la forma de proteger a los estadounidenses vulnerables.

Es por eso que estamos aquí en el gran estado de Florida para la audiencia de hoy.

Nuestro estado es el hogar de ás de 4 millones de personas mayores. Es un punto de acceso para los jubilados y, desafortunadamente, actividad fraudulenta.

Es por eso que he convertido en una prioridad trabajar con las fuerzas del orden locales, estatales y federales, grupos comunitarios y nuestros lφderes estatales para combatir el fraude de frente.

También debemos analizar detenidamente de dónde provienen muchas de estas estafas. Y esto no se puede hacer solo a nivel local, tenemos que hacerlo a nivel federal.

Cada vez más, estamos viendo operaciones de fraude transnacionales coordinadas, especialmente de la China comunista y otros adversarios extranjeros, y no olvidemos que son nuestros adversario, la China comunista es un adversario, si compras algo de los comunistas de China, estás ayudando a un adversario.

Estos no son incidentes aislados. Son operaciones a gran escala que se ejecutan desde llamadas en el extranjero, centros de investigación, a menudo con el conocimiento, o incluso la protección, de regímenes como el Partido Comunista Chino.

Estos grupos utilizan datos robados, tecnología de inteligencia artificial y criptomonedas para explotar Americanos.

Esto es más que un problema de proteccion al consumidor; es una preocupación de seguridad nacional para nosotros. Es necesario tratarlo como tal y responsabilizar a estos delincuentes por permitir actividades que perjudican a las personas mayores estadounidenses.

He presentado la Ley STOP Scammers. Este proyecto de ley le da al Departamento del Tesoro la autoridad para designar formalmente las redes de estafa como ″Amenaza financiera extranjera″ y congelan sus activos, cortan sus líneas de comunicación y bloquean su acceso a nuestro sistema financiero. Una cosa que tenemos que hacer, y he hablado con el director del FBI Kash Patel y la procuradora general Pam Bondi sobre esto, tenemos que asegurarnos de que nuestros recursos se centren en lo que tenemos que hacer a nivel federal, y no en lo que tenemos que hacer sobre las cosas a nivel local que pueden hacer los departamentos del alguacil.

Si una organización externa se aprovecha de las personas mayores estadounidenses, deben ser tratadas con la misma gravedad y sanciones que cualquier otra amenaza a nuestra seguridad nacional. Es decir, exactamente lo que la Ley STOP Scammers nos permite hacer.

Hoy, escucharemos a los líderes que están combatiendo este problema en la primera línea de nuestras comunidades. Escucharemos cómo están trabajando para combatir el fraude y proteger a nuestros adultos mayores.

Nuestro objetivo hoy es simple: educar al público sobre este importante tema y comenzar a eliminar el estigma asociado con la denuncia de fraudes y estafas cuando ocurren. Hay mucha gente que se avergüenza y no quiere denunciarlo, no quiere contarlo a sus familias y claramente no quieren decírselo a la policϕa.

Escucharemos a nuestros líderes comunitarios sobre cómo lograr esto, qué medidas podemos tomar para proteger a nuestras poblaciones vulnerables contra los estafadores, y cómo podemos empoderar a nuestros adultos mayores para que reconozcan estas amenazas.

Las personas mayores merecen sentirse seguras al contestar el teléfono, abrir su correo electrónico y confiar en las personas que los rodean.

También merecen sentir que serán escuchados y que sus preocupaciones son válidas cuando denuncian el fraude a las autoridades locales.

A menudo, es la policía local la que tiene que recoger los pedazos apoyando víctimas, investigando estos crímenes y tratando de evitar que vuelvan a suceder.

Esta es una de las razones por las que la miembro de Alto Rango Gillibrand y yo, nos unimos al Senador Britt para introducir la Ley GUARD. Este proyecto de ley apoya las investigaciones policiales sobre estafas contra los jubilados y amplía el uso de las subvenciones existentes para perseguir las redes de fraude.

El trabajo que realizan nuestras fuerzas del orden público en la identificación e investigación de estafas contra los jubilados son cruciales para esta lucha.

Our next witness is Jeff Johnson, the Florida State Director of AARP. Thank you, Sheriff.

STATEMENT OF JEFF JOHNSON, STATE DIRECTOR, AARP FLORIDA, ST. PETERSBURG, FLORIDA

Mr. JOHNSON. Thanks for the opportunity and for inviting us to testify today. My name is Jeff Johnson. I am the State Director for AARP Florida.

AARP advocates for more than 100 million Americans age 50 and older, including 10 million here in the Sunshine State. AARP has long worked to educate consumers, support victims of fraud, and improve detection and prevention across industries, including through our Fraud Watch Network, our Bank Safe Program, and our advocacy work in the states and at the federal level.

Fraud in America is at crisis levels. Floridians reported the theft of over $1 billion from fraud in 2024, over 1/3 of which was stolen from adults aged 60 and older, and that is very likely a low estimate due to underreporting caused in part by the stigma and victim-blaming associated with fraud. While our society treats many victims of other crimes with compassion, we tend to place responsibility on the victims of fraud who fell for a scam, blaming victims for not being smart enough or paying close enough attention in the first place, and this works in favor of criminals who know that most of these crimes may go unprosecuted.

Older Americans aren't just losing their retirement savings from fraud. In some cases, they are even losing their homes. Just last month, AARP's Fraud Watch Network helpline received a report from Edward, a Florida man in his 60's who had the entire proceeds from the sale of his home stolen by cybercriminals, more than $400,000 in total. With all his money gone, this older Floridian went from selling his home in order to downsize to facing the threat of homelessness in a matter of seconds.

While I know that you and the rest of the Committee are very familiar with the work that AARP does at the federal level of policymaking, and I would like to thank you in particular for your sponsorship of the GUARD Act as just one example of the federal policy addressing fraud, I would like to focus on the work we are doing here in the Sunshine State in today's remarks.

AARP Florida plays a key role in educating Floridians about the latest scams and frauds and how to prevent them. We don't do this work alone, however. Local law enforcement agencies are key allies in education, sharing our resources while we in turn highlight their services and sharing the excellent work that they do. For example, our team recently showcased the SafetyNet program of Walton County's Sheriff's Office, which offers isolated residents in the Florida panhandle with a lifeline, social connection through the Sheriff's Office that provides meaningful health and safety protections, while reducing residents' risk for potentially devastating cases of fraud and exploitation too often caused and/or concealed by social isolation.

AARP hosts fraud prevention events in communities across the state, including shred events that allow residents to safely dispose of sensitive information that might otherwise fall into the hands of fraudsters. Often these events are paired with educational seminars and trainings. Within the past year, AARP has hosted two different fraud prevention summits in partnership with the U.S. De-

partment of Justice here in Florida, one in the Villages and then one in Century Village here in south Florida.

Even the best education, though, is only a piece of the puzzle. AARP Florida has supported state laws and regulations tackling real estate scams, suspicious financial transactions, and gift card fraud, providing model policies and practical protections that strengthen safeguards for consumers at the state level. We are now taking the fight against fraud to the local level, working with several local governments to tackle cryptocurrency kiosk fraud.

Addressing fraud requires more than piecemeal solutions. It demands a whole-of-society approach. Even though there is much work to do, Florida is an example of what this type of comprehensive approach could look like. AARP Florida is working directly with allies to provide real-time education and to support our neighbors and loved ones who are at risk of being scammed. We also are working with policymakers at all levels of government to improve laws and regulations to protect consumers and prosecute fraudsters, and we work with law enforcement agencies across the state that have identified the dramatic scope and impact of senior fraud on their communities and who are fighting back. There is much more work to be done, but we all recognize the crisis, which is the first step toward turning the tide.

Thank you, Chairman Scott, for bringing attention to this important issue, and we look forward to continuing to work with you to protect Florida seniors.

Chairman SCOTT. Thanks. Let me just brag about Jeff for a second. Jeff has spent years leading efforts to empower older Americans with the tools they need. AARP does a great job. This fraud watch network has become a lifeline for many seniors, so they do a great job, and Jeff is committed to this every day, so——

Mr. JOHNSON. Thank you.

Chairman SCOTT. You should be Governor because, as Governor, you get to meet everybody in the state, and you get to build great relationships, and you find good people doing a lot of great things, so I always want to call out my friend Rene, because Rene was campaigning when no one knew me in the state, and everybody knew Rene, so I just tried to stand next to him whenever I was in Hialeah.

Mr. JOHNSON. Thank you, Mr. Chairman.

Chairman SCOTT. All right, now our next witness, Kathy Kraninger, the president and CEO of the Florida Bankers Association, she brings a wealth of experience in financial policy and consumer protection, having served in senior leadership roles in both government and the private sector. Under her leadership, the Florida Bankers Association has worked closely with banks across the state to protect older customers from fraud and scams through training, technology, and increased awareness for both customers and employees. Thank you for being here, and by the way, Kathy doesn't have just great relationships here in Florida. She has great relationships in D.C. also and did a great job when she was up in D.C.

You can begin your testimony, please.

STATEMENT OF HON. KATHY KRANINGER, PRESIDENT & CEO, FLORIDA BANKERS ASSOCIATION, TALLAHASSEE, FLORIDA

Ms. KRANINGER. Thank you, Mr. Chairman.

Chairman Scott, on behalf of the Florida Bankers Association and our more than 150 member banks across the great State of Florida, I am honored to appear before you on this crucial topic. Bankers are on the frontline of the fight against fraud, working to protect our customers against scams, identity theft, and cybercrime, and this Committee, and certainly you, Mr. Chairman, as you have said, know well that the level of fraud and scams now constitutes a national crisis.

While some of the most troubling cases affecting the most vulnerable among us, such as older Americans, who are the focus of this Committee, no one is immune from the barrage of attempts via every mode of communication in our modern society. It is a game of numbers. The sheer volume and ease of attempts means more success for the bad guys. Scammers are approaching targets through email, phone, text messages, social media channels, social media ads, just to name a few of the avenues, and the technology advancements, as we know, like deepfakes, enable more sophisticated deceptions.

Right now the bar is fairly low. The scammers can be so successful that, as we have already heard, transnational criminal organizations are heavily involved in these types of frauds, so much so that Bankrate recently found that one in three Americans experienced some type of financial fraud or scam in the past year, and 68 percent reported that they had experienced one in their lifetime. My written testimony and the testimony submitted by my fellow witnesses outlines the problem and the heartbreaking stories of those directly affected.

Bankers are deeply concerned about these trends. We know our customers and are doing everything possible to prevent the loss of their hard-earned savings, as well as the emotional and personal impacts that scams have on victims. Banks appropriately have made significant investments in detecting suspicious activity and acting to stop fraud, as permitted by law. We are advocating for state-level hold laws and have worked with AARP to pass one in Florida. With the right protections, these laws allow banks to delay or hold transactions when there is suspicion of elder financial exploitation. In addition, we encourage customers to provide trusted individuals that banks can contact in the case of suspicious activity.

Financial education also plays a significant role in countering fraud, and financial institutions are consistent in providing customer education and employee training. With campaigns like ″Banks Never Ask That,″ as the Sheriff outlined, many of the things that you should never provide to anyone who calls you cold, and Practice Safe Checks. Bank employees are doing so much, yet the hardest piece of this puzzle is often convincing customers that they are being scammed. Ultimately, banks cannot stop those insistent customers from doing what they want to do with their own money.

What more can we do? The Florida Bankers Association advocates for a national strategy that will tackle fraud and scams from all angles, including cutting off those communications channels to targeted victims, bolstering public education, and ensuring prosecution of criminals. As a society, we have to look for opportunities to intervene before the point of payment.

The banking industry has encouraged and supported the Federal Communications Commission in its efforts to combat fraud perpetrated over our telecommunications systems, including development of a scam database and requiring caller ID authentication solutions on non-Internet protocol networks. Telecommunications, big tech, and social media companies need to do more to raise the bar on the ease for scammers' initial contact with their targets. Selling services to consumers to block certain approaches like communications from overseas that they don't want and don't expect, as well as engaging in voluntary best practices to flag potential scam accounts or ads for customers, can only help.

Government agencies need to have clearer lanes in gathering and sharing actionable, up-to-date information on the typologies, patterns, and characteristics that they see scammers employing, and partnership with law enforcement at the local and state and federal levels is absolutely essential, as you have already heard. The FBA is working with the Florida Attorney General's Office to explore establishing a financial crimes intelligence center at the state level that would be dedicated to financial crimes identification and information sharing, like one employed in Texas about three years ago, that is really seeing success, and the effort would build on the great work already done by the Cyber Fraud Enforcement Unit.

Fraud is not just a banking problem. It is a societal threat that requires coordinated action, as we have been saying. Florida's bankers are committed to protecting our customers and our communities, but we cannot do it alone, and we are incredibly grateful for your leadership, Chairman Scott, and certainly for the partners who are around this table in the efforts that they have undertaken to make sure that the public is aware and to shine a light on these horrific scams.

I look forward to answering your questions and appreciate the opportunity to be here.

Chairman SCOTT. Thanks, Kathy.

Our final witness is Brandy Bauer, the Joint Center Director for the State Health Insurance Assistance Program Technical Assistance Center, easy name, and the Senior Medicare Patrol National Resource Center. She has led national efforts to equip seniors with the knowledge and resources they need to spot, stop, and report Medicare fraud. Through the Senior Medicare Patrol, she helps empower older Americans and their caregivers to safeguard their benefits and personal information, often serving as the first line of defense against scammers.

Brandy, first off, thanks for your work, and thanks for joining us.

STATEMENT OF BRANDY BAUER, JOINT CENTER DIRECTOR FOR THE STATE HEALTH INSURANCE ASSISTANCE PROGRAM (SHIP) TECHNICAL ASSISTANCE CENTER SENIOR MEDICARE PATROL (SMP) NATIONAL RESOURCE CENTER, WATERLOO, IOWA

Ms. BAUER. Thank you, Chairman Scott. Thank you for inviting me here today on behalf of the Senior Medicare Patrol Program.

The nation's 54 Senior Medicare Patrol, or SMP programs, are managed by the U.S. Administration for Community Living with the mission to help empower and assist people to prevent, detect, and report Medicare fraud, errors, and abuse. Medicare fraud is a particularly insidious form of financial scam because, unlike other fraud schemes targeting an individual, the government and American taxpayers all pay the price. It is also challenging to detect Medicare fraud in real time, as there can be weeks or even months between when Medicare is falsely billed for services and when an enrollee sees that charge show up on their Medicare summary notice or plan's explanation of benefits.

The Senior Medicare Patrol program model is one of prevention. SMPs educate millions of Medicare beneficiaries each year on how to guard their personal health information, scrutinize their medical statements and bills, and subsequently alert the program to any suspicious activity. The SMPs report cases of possible fraud, errors, and abuse to the Centers for Medicare and Medicaid Services and HHS Office of Inspector General, who take up the investigation.

Here is just one real-life example of how this work plays out. Recently, a gentleman from Walton County, Florida, was looking at his Medicare summary notice and discovered charges for urinary catheters and glucose monitoring supplies, equipment that he neither needs nor ever received. He reported this to the Florida Senior Medicare Patrol, who were able to help him get a new, uncompromised Medicare number. Yet Medicare had already paid over $15,000 for these fraudulent charges.

This beneficiary was observant. Think how many times this scenario plays out across Florida and the country and goes undetected. As such, it is hard to get a concrete calculation of how much Medicare fraud costs Americans each year, but estimates put it in the tens of billions of dollars.

Because the Senior Medicare Patrol relies heavily on trusted volunteers from the community, in many cases older adults themselves, the SMP program is often on the forefront of detecting emerging fraud trends. SMPs were among the first groups to spot unusual activity around fraudsters offering COVID0919 test kits in exchange for personal or medical information. Other emerging schemes the SMPs have helped identify include genetic testing scams, hospice fraud, and most recently, schemes related to remote patient monitoring and wound care.

In addition to costing Medicare billions of dollars, some of these schemes can cause real patient harm, such as when a person falsely enrolled in hospice may be denied coverage for services that fall outside of palliative care.

The Senior Medicare Patrol is an Older Americans Act success story. First authorized under the OAA in 1997, the SMPs have provided outreach, counseling, and education about Medicare fraud to

millions of older Americans. Since their creation, expected recoveries to Medicare and Medicaid attributable to the SMPs equals more than $287 million.

But Medicare fraud doesn't exist in a vacuum. People vulnerable to other forms of financial exploitation may be at risk of unknowingly sharing their medical identity with health insurance fraudsters. Many of the same prevention strategies that we have heard from the panel are relevant here as well, such as encouraging people with Medicare to guard their medical identity just as they would their Social Security or banking information, hang up on unsolicited calls, and report suspicious activity to the authorities. The Senior Medicare Patrol's efforts not only serve to enhance the financial, physical, and mental well-being of older adults, but also to preserve the integrity of Medicare.

I would like to thank the Chairman and the Senate Aging Committee for including our program in this important conversation today.

Chairman SCOTT. I have some questions. Sheriff, do you believe penalties for elder exploitation are strong enough to deter criminals?

Ms. CORDERO-STUTZ. No, I actually believe that it is the fact that there is a lack of that pressure of real threats against committing these crimes that encourages this behavior. We need to increase the penalties on these kinds of crimes.

Chairman SCOTT. Kathy, so if I got a letter from some law firm from Canada, and they said that they represent somebody that died, had the same last name as mine. They weren't sure that they were related to me, but maybe it was like $10.5 million dollars. I could get half of it and they get the other half, and then I looked on the website, and it looked like a real law firm, but it had nobody's name. Is that something I should be concerned about?

Ms. KRANINGER. The answer is definitely yes. Mr. Chairman, as you well know, if it sounds too good to be true——

Chairman SCOTT. Five and a half million bucks.

Ms. KRANINGER. I know. If it sounds too good to be true, it probably is. I feel like so many of us need that reminder, but it is really the barrage of things that come at us every day and the distractions in modern society, and then you do talk, obviously, with those who are vulnerable and with diminished capacity. That is just a different world.

Chairman SCOTT. Wouldn't it just be a potential upside? Would I have to write a check or something?

Ms. KRANINGER. This is how they string you along, as you well know, so they will tell you that this money could be coming at you, but then, of course, you have to pay some kind of fee to start the process going, and that is absolutely the way the scammers hook you.

Chairman SCOTT. I got a letter just like that, same last name, and I looked up the law firm and it had the law firm, but had no lawyers listed, right? I just gave it to my general counsel. I mean——

Ms. KRANINGER. Yes, imposters issues are huge. I mean, it is so easy. Well, frankly, in this state, too, and in general across the country, it is so easy to set up a corporation, too, so there is a lot

of fraud happening in even business setup processes too, so you can pretend—you are essentially a real corporation. You have been approved or you set up a shell and you use that, again, to scam people. It is very concerning, and it is too easy.

Chairman SCOTT. Jeff, those nice texts I get that say I owe money for E-ZPass——

Mr. JOHNSON. We were just talking about that.

Chairman SCOTT. That is not fraud, is it? I just send them my credit card——

Mr. JOHNSON. Right.

Chairman SCOTT Right? Is that what I am supposed to do?

Mr. JOHNSON. Senator, please don't do that. You know, one of the things that has been fascinating has been the development of kind of scammers on-the-ground intelligence. They jump on a new scam, and then it explodes, and you will be driving on a toll road and start getting texts even if you are not in that state, even if you are not in your car, that look like maybe they could be correct, and yet you realize if you go check it out at the source, that SunPass is not hunting people down by text in order to collect their tolls, and if you pay attention, sometimes you will see that the address, though it can be deceptive, often is coming from an international number, to go to your point that this is not just a domestic issue.

There are opportunities to learn, but every time we close off one scam, it seems like folks just figure out what is the next way that I can get your hard-earned money.

Chairman SCOTT. Brandy, when some provider does what—you know, as an example you had, who pays for that?

Ms. BAUER. Medicare, but all of us.

Chairman SCOTT. Right.

Ms. BAUER. At the end of the day, all of us are American taxpayers, and we will see that, you know, carried on to us through higher premiums, through higher cost of services.

Chairman SCOTT. First off, we all know the Medicare trust fund is going to go bankrupt in six or eight years, right?

Ms. BAUER. Yep.

Chairman SCOTT. Then on top of that, what we have watched is we have watched seniors, their premiums are continuing to go up.

Ms. BAUER. Right.

Chairman SCOTT. If there is X dollars of fraud, we are paying for it.

Ms. BAUER. Exactly.

Chairman SCOTT. It is not free.

Ms. BAUER. Exactly. That solvency date, you know, it keeps moving because the more the system is scammed, you know, the less solvent it is going to be.

Chairman SCOTT. Right. Mr. Johnson, one thing I have tried to do is try to get help close to community rather than—there is a bureaucracy in D.C. I don't know if you guys knew that——

Mr. JOHNSON. Oh, well——

Chairman SCOTT. From AARP's perspective, how does the GUARD Act strike the right balance by empowering local agencies and community groups without relying on Washington to do it all?

Mr. JOHNSON. Thank you for asking that question, Chairman Scott, and I think that the value that we see in the GUARD Act

is that it does empower local law enforcement. One of the things that we notice is that on the policy side, in addition to being wonderful fellow educators to help empower people to fight fraud, it is local law enforcement that sees what the problems are.

There are often cases where—and I will use cryptocurrency kiosks as an example—where at the federal level, there is some knowledge that there is potential use of those as fraud, just as gift cards in the past have been used as fraud. At the state level, there is some knowledge of it, but you go talk to a local sheriff or local police chief, and they will tell you stories of people who have lost thousands and thousands of dollars.

They also will help identify what are the ways that we can rein that in without necessarily, you know, limiting reasonable use of those, you know, kiosks. How do we make sure that the fraudsters aren't using them or other criminals? That is the other thing that we have learned is that local law enforcement has noticed that cryptocurrency kiosks tend to be popular among drug dealers in some communities.

Well, it is that community-level information that is really critical, right, in order to build the right solutions and then also to build the momentum to pass things at the state and the federal level, so thank you again for empowering those local law enforcement agencies with opportunities to really do more of this because I know that they are already stretched.

Chairman SCOTT. Sheriff, do you think most local law enforcement has the resources to go talk to a social media site to say, hey, you need to take this down because they are fraud? Are they responsive all the time?

Ms. CORDERO-STUTZ. We are always challenging law enforcement when it comes to resources, so we could always use more resources. That is the honest truth, and additionally, we do often get pushback from some of these organizations, whether social media platforms or networks, and it often feels as if more protection is afforded to those who are misusing the platforms than to those who are trying to protect people. I think that is a challenge that we have to continue to, you know, attack head on.

Chairman SCOTT. It is not easy to get them to—when you are convinced that there is fraud, it is not easy to get them to stop.

Ms. CORDERO-STUTZ. Absolutely. It is very difficult. They make it a multilayer process, and sometimes you just can't even get in touch with a human being.

Chairman SCOTT. Oh, so they don't have a phone number you can call that makes it really easy?

Ms. CORDERO-STUTZ. Yes.

Chairman SCOTT. Like when you want to unsubscribe.

Ms. CORDERO-STUTZ. Correct. Correct.

Chairman SCOTT. Ms. Kraninger, talk about the holdout? I mean, just tell me, you know, what the problem is. Somebody sends the money, and then they figure out that, oh, man, I just made a mistake. How does the bank deal with this?

Ms. KRANINGER. At least it is an option with respect to these hold laws, and that is possible because the banks, as I noted, have really pretty sophisticated systems on transactions. They understand what is normal behavior for this client, what is not normal

behavior. You know, suddenly a senior is sending money again to an overseas wire account and they have never done that before, and it is usually, again, the first drip or you let the first drip go, but then you say, oh, my gosh, there is another one that is coming now. First one was 500 bucks, the next one is 20,000. You know, that seems pretty unusual.

That is where, with the right law in place, as we have in Florida, a bank can stop that transaction and not even allow the wire to go forward, but then it really is a very manual process of convincing that client that this is probably not——

Chairman SCOTT. Do they complain that you—I want to send that fraudulent amount, right?

Ms. KRANINGER. Yes.

Chairman SCOTT. You are convinced, but they are still convinced you have to send it, right?

Ms. KRANINGER. Yes, that is exactly what happens. Again, you talk about the heartstrings that scammers are pulling on—I mean, all of us are vulnerable to that -- you know, it is my grandson who really needs help or, you know, the prince actually. The prince scam went around for a long time too, so this is someone who really needs my help or, again, this person is going to come and marry me in the United States if only they can get this amount of money to buy the visa, and so all of those kinds of stories, the bank tellers and managers and client services folks have heard it all, and it really is convincing that person that is a challenge.

Oftentimes, unfortunately, it goes forward or, again, the option that the bank has to take if there really is no other way to stop it is to close the account, but then there is no information-sharing mechanism either because we are not allowed to for, I mean, good regulatory reasons. Then that customer goes to another bank, and the whole cycle starts over again, and that is the thing that we do see.

The hold law does—hopefully, again, it stops the process, forcing people to stop and think and pause and say, wait a minute, you know, this really doesn't make sense. That is an important part of what the hold laws do, but it is not the end-all, be-all, and we really just have the initial data on how it is working, and we are looking to get more data to get that improvement and to work with law enforcement, as those things get reported to FinCEN as suspicious activity reports and otherwise, that we can tie it to transnational organized crime and that we can tie it to law enforcement cases.

Chairman SCOTT. You work both at the federal and state level. Is it a lot easier sometimes to get stuff done at the state level?

Ms. KRANINGER. It absolutely is because I am finding—I spent my career, as the Chairman well knows, in Washington, DC., and moved to Florida a year and a half ago, and things can definitely move. Yes, things can move faster at the state level. It is true. It is true.

Chairman SCOTT. Yes. Ms. Bauer, as Joint Center Director, can you explain how the State Health Insurance Assistance Program helps seniors navigate the Medicare options while avoiding fraudulent actors?

Ms. BAUER. Yes. Every state has a State Health Insurance Assistance Program. They go by different names. Here in Florida,

they are called SHINE. That is a federally funded program that helps people to explore their options for enrollment and coverage and affording Medicare and really can help anyone with Medicare family members, caregivers to examine their coverage, learn how to read your Medicare summary notice or your explanation of benefits so you actually know how to look out for those potentially fraudulent charges and also to get you enrolled in the plan that is going to be best for your financial and physical needs.

Chairman SCOTT. How do they find you?

Ms. BAUER. Here is the thing. You have to find them. The SHINE is sort of the best-kept secret. I know that they only serve a very small percentage of, you know, the 67 million people on Medicare, but there is one in every community, and we certainly encourage you—if you go to SHIPhelp.org, you can find your local office.

Chairman SCOTT. Sheriff, you have built really good relationships—before you were sheriff and while you are sheriff, you have built really good relationships, so what are some of the relationships that that you rely on when a senior—you know, one, you are trying to educate people; and two, when somebody calls you, what are some of the relationships you have?

Ms. CORDERO-STUTZ. Yes, I think a lot of our community support organizations that already have—our seniors are tapped into them already, so I think for us in law enforcement, being able to have kind of like an area that we can always go to and have an audience already built in, and also, because they are already reporting to some of these community organizations as a community, a senior community, you will hear about the crime occurring in those rooms, and so by just being present, it allows us to hear something, I go, wait, time out, that doesn't quite sound right.

Also creating those relationships with our community leaders and organizations allows them to be able to pick up the phone when they hear something and get us the information. The sooner we identify the frauds, the sooner we can share with individuals and kind of break that trend, and that is key, and you are right. The new one is going to pop up after, but we are hopeful that as we continue to educate our community, they will be able to see things from a different lens.

Chairman SCOTT. My experience is there are way more senior centers here——

Ms. CORDERO-STUTZ. Yes.

Chairman SCOTT. Than any place in Florida so——

Ms. CORDERO-STUTZ. Yes.

Chairman SCOTT. Which I think probably helps everybody that wants to try to get something done and educate people.

Ms. CORDERO-STUTZ. Yes.

Chairman SCOTT. What are some of the most recent scams that you have seen?

Ms. CORDERO-STUTZ. Well, AI-generated voice calls, so you will get a robocall that sounds just like a grandson or granddaughter saying that they are in need of help immediately. One of the recommendations that we make in law enforcement is, is every family should have this very tough conversation and say there is a safe

word, a family word that if you are in trouble, you need to use, so that way it will protect the rest of the family from being scammed.

You cannot tell the difference. The voice, it will sound exactly like your loved one.

Chairman SCOTT. Yes, somebody called me to get me to—they left a message to get me to accept somebody at the White House. It sounds just like them.

Mr. Johnson, what is the latest you are seeing as far as scams?

Mr. JOHNSON. Definitely the evolution of AI has made it much more difficult to suss out who is a scammer and who is legitimate. We see romance scams quite a bit among older adults and people of all ages, again, using AI and deep-fake technology. I think I saw something recently about a number of people losing money to fake Keanu Reeves, not actually Keanu Reeves trying to date you, but a scammer somewhere, and it preys on the loneliness that many people have in older adulthood, so they look for companionship. It may not even be romantic, but they make friends with somebody online, they might have a couple of calls, and then it becomes something that either becomes extortion or else just outright fraud and we have seen over the last couple of months, our Fraud Watch Helpline has had, I think, half a dozen people who have lost $100,000 or more to these scams.

Chairman SCOTT. Right.

Mr. JOHNSON. Yes.

Chairman SCOTT. Kathy, what is your latest?

Ms. KRANINGER. I can certainly add on that. I will say the romance scams are the top of the list, and it really gets you to how lonely and disconnected people are today, which is concerning, and being in a community like this and seeing how connected everyone, you hope that people can overcome it.

Investment scams are also big. It gets to the point that you raised about the law firm and the money that suddenly could come your way.

Chairman SCOTT. I made a half million bucks.

Ms. KRANINGER. Yes. It sounds too good to be true, so there are a lot that are crypto-related in particular. You are basically setting yourself up on what looks like a legitimate exchange, and they are giving you, you know, a reward for signing up, and they are hooking you and taking, again, an initial amount of money where you are buying the tokens. You can see that the investment that you have just made is increasing, and so, again, they are dripping it to you and trying to get you to put in more and more money.

The bank will notice, again, that amount of activity and start to say, is this a legitimate entity? No, it is not, so they will contact you, and you will say, no, but this is my investment, and we will say, okay, try to withdraw the money, and they will say, well, I don't want to do that, or they are telling me there are going to be penalties. Just try to do it. You cannot withdraw the money. They literally shut down your account and disappear because, again, it is all coming from overseas, and it is transnational criminal organizations, so that is a big one right now.

Chairman SCOTT. Ms. Bauer, what is the latest scam you have heard?

Ms. BAUER. I feel like there are so many, as the sheriff mentioned, you know, these imposter calls. A lot of older adults get calls from an agency that they believe is Medicare calling them and saying, hey, you need to get your new Medicare card with a chip in it or something like that, and some of them utilize AI to actually provide enough information like, hey, your name is John Doe, your Social Security number, your Medicare number, and then the person confirms, and that information, you know, is carried forward.

Another one we are seeing is fraudsters that really tap into very expensive durable medical equipment, so something we are seeing more of is urinary catheters, for example, where they are billing for tens of thousands of urinary catheters and people who don't even need that, glucose monitoring equipment. Another one very recently, wound care. There is a new product on the market that is quite expensive that is for very specialty wound care. Fraudsters are finding that code and billing Medicare tens of thousands——

Chairman SCOTT. They just put it on the bill?

Ms. BAUER. Yes, just put it on the bill.

Chairman SCOTT. Then nobody checks?

Ms. BAUER. Nobody checks.

Chairman SCOTT. Yes.

Ms. BAUER. Yes.

Chairman SCOTT. Because there is probably no copayment or something.

Ms. BAUER. Or the copayment, you don't get that notice for like several months down the line. You know, the charge has already gone through and been paid.

Chairman SCOTT. Then they are going to expect you to pay it.

Ms. BAUER. Yes.

Chairman SCOTT. Yes. Can you each talk about some success story? Rosie, you want to start?

Ms. CORDERO-STUTZ. Okay. Well, I think I would argue more because it was a successful campaign that we initiated.

Chairman SCOTT. Yes.

Ms. CORDERO-STUTZ. We went on a very proactive social media campaign to educate specifically our elderly community on these scams, and we encouraged them to reach out to us directly to provide input if they had heard of any other scams, again, attacking that, you know, get to it as soon as possible, and as I was out in the community, you know, I hear it from them, like, that was great, that made me stop and think the next time someone, you know, called me. Unfortunately, those calls come way too often for all of us.

Yes, I think that being proactive, listening to what is going on, and that educational piece, where are they turning to? Where is our senior community turning to for their facts about how they can be scammed? We need to make that easier. We need to make it much more readily available to them.

Chairman SCOTT. Mr. Johnson, any success stories?

Mr. JOHNSON. Yes, I think so. I would say what does success look like is important, right? For us, I think it is really about empowering each other to serve as neighbors who advocate for each other and to do it humbly, so, for instance, we do fraud education summits and we have volunteers here and staff members who do this

in community, as well as working with law enforcement, U.S. attorneys, certainly would work with banks, anybody who has good information we want to get out, and what we notice is once people have gotten a good message, they get really excited about catching the next scammer. Oh, look, I got this. Oh, look, here is another one, and instead of spreading the word about the latest scam as somebody who is being scammed, they are spreading the word to their friends and neighbors about the last one that they almost fell for, that they almost were scammed by, and how we try to make sure to protect each other.

The other one related to that kind of empowering each other, we have worked with financial institutions at the national level, as well as in Florida, on a program called BankSafe to try to prepare the frontline, the tellers, with the sorts of kind of psychological behavioral tools to help somebody that you think is being scammed because, as Kathy said, this is something that is a very difficult conversation, and what we found is that that training makes those tellers—those workers who go through that training with 14 times more effective at helping prevent somebody who is being scammed from actually going through with it, so knowledge really is power.

We also need to recognize that we all have to be vigilant because even if you are a fraud education expert, it doesn't mean that you are invulnerable to the next one that comes down the pike.

Chairman SCOTT. Kathy?

Ms. KRANINGER. Well, building on what Jeff just said about training and what the frontline bank tellers do and others who are interacting with clients, it is the trusted contacts, or, you know, again, similar to the safe word, having a trusted contact program and encouraging, frankly, all your family members to provide that to the bank because many situations where the senior is showing up at the bank, again, wanting to withdraw that $10,000 so they can go to the crypto kiosk that is down the street, and that is what they have been told to do, and they are coached, again, by these scammers about what to say, what is suspicious, what is not, you know, the urgency of the situation.

Having that trusted contact in the account allows the bank employee to say, you know, have you talked to your son or daughter? Do they know about this? Again, probing and actually trying to contact that person in real time, that has prevented some from losing funds.

There was a case, again, down in Miami here that we talked about recently was basically, okay, you want $10,000. Well, the limit is $500 today, so we are going to give you your $500 and calling local law enforcement to meet this gentleman, you know, at the kiosk to have law enforcement also intervene to say, let's get some more voices in front of this person to hopefully stop them from doing it, and so he actually only lost $500 and realized it was a scam, so those types of things are happening, you know, every day.

I would say at the national level, there is a lot happening around check fraud in particular. Every avenue of payment, there is nothing that isn't——

Chairman SCOTT. How are they doing that?

Ms. KRANINGER. Check fraud, there are massive things that are happening actually through the Postal Service too. We have been

partnering with the Postal Service Inspection Force—stealing. I mean, having postal keys is now a crime in Florida. We worked on that last year.They were breaking into the boxes and literally taking all the mail and then just taking all the checks and, again, washing checks again. I mean, similar to what we saw 20 years ago, it is back, and so there is a lot around paper checks. This is why the Federal Government and Treasury in particular is requiring verification of Treasury checks. The President signed the executive order to really phaseout checks. Those kinds of things are happening.

I mean, the amount of check payment has gone down. I don't remember the numbers off the top of my head, but in the order of 40 percent, 50 percent, but the amount of fraud has gone up, so it is just taking the easiest route, but check fraud, since we haven't talked about it yet, is still an issue.

Chairman SCOTT. Yes. Any success stories, Brandy?

Ms. BAUER. Yes. I mean, the Senior Medicare Patrol, although it is a program focused on prevention, there is a lot of reporting up to the HHS Office of Inspector General who goes on to investigate. Each year the OIG within HHS produces a report where they talk about the Senior Medicare Patrol and the recoveries that they were able to eventually make for Medicare on behalf of the project. Last year, it was $35 million. The year before, it was $111 million.

It is challenging with Medicare fraud because it is usually multi-years investigation on the part of OIG and then having to attribute it back. You know, we are very happy that we are able to see things on the ground, report it up, and eventually see justice served.

Chairman SCOTT. Jeff, can you speak about the role of digital literacy in helping seniors stay safe online?

Mr. JOHNSON. Yes, absolutely, and as check fraud comes back, it is another emphasis for people to do a lot of their financial transactions online, so to be able to do that well, you need functional digital literacy.

One of the things that AARP is proud of is here in south Florida there is OATS, Older Adult Technology Services, which is an affiliate of AARP, has a training center. We also license for free training on digital literacy all across the state, all across the country. That just helps people make the next step in learning how to use the tools that are available to them safely because, otherwise, to your point, Mr. Chairman, there is too much opportunity for somebody who is a little unsure or unpracticed in using a particular, you know, website with verification and what information you put in, what do you not, those sorts of things, for a scammer to set up a pretty good-looking fake, just like the law firm in Canada that is hunting you down, and get your Social Security number out of it or get your bank routing number out of it, and then, of course, a whole cascade of frauds and scams come from that.

To your point, critically important for all of us to stay up on the latest technology, but particularly those who didn't grow up with a phone in their hands, to become more and more comfortable knowing what is safe to do and what should set off some alarm bells.

Chairman SCOTT. Sheriff, do you have any special training for your officers to try to deal with elder fraud?

Ms. CORDERO-STUTZ. Yes, we do. We actually have an entire unit dedicated to investigating those types of crimes. For us, obviously, I mentioned in my statement that we have such a large population of seniors that live here, so obviously, I think that we are in a special place to be able to really affect that community. Not only applying dedicated resources and training to these kinds of investigations is key, but working with our partners in trying to prevent it.

He gave me a great idea. I think we are going to reach out. I see a community event where you guys can bring that to our community centers who might not otherwise even know. It is this collaboration, I think, that will make us all be successful.

Chairman SCOTT. Kathy, what are the Florida banks doing to train their frontline employees? What is an example of what they are doing?

Ms. KRANINGER. Well, as Jeff mentioned, BankSafe, too, that is a big effort, but there is constant training, as you know. Banking is a heavily regulated industry for good reason. You are shepherding and holding people's money and their hard-earned——

Chairman SCOTT. Right.

Ms. KRANINGER [continuing]. savings, so there is extensive training for bank employees, frankly, at all levels. Again, you get to digital banking now, and while seniors still tend to come in person to the bank branches, most people are not coming to the bank branch, so you have got managers that may be supporting them on the wealth management side, and so there is training at every level of bank employees around how to interact with customers, how to identify suspicious activity, what to do in terms of reporting, and even, you know, strengthening the law enforcement relationships locally are all pieces of training happening.

It is an awkward conversation, as I noted, and so, as with other things in training, doing some role-playing around that is also part of the training at a lot of the institutions to try to get employees more comfortable with, you know, having what are, again, challenging conversations with customers that do not want to hear the message that the employees are delivering.

Chairman SCOTT. Brandy, what can this Committee do to amplify your efforts and ensure every senior's access to fraud protection?

Ms. BAUER. I think that the Committee is doing a fantastic job in elevating just the variety of fraud schemes that are out there, all of which kind of play into Medicare fraud. One thing I think we would love to see more of is awareness and promotion around the idea that medical identity is as important as personal identity, as banking information, and we need to do a better job of preventing medical identity theft and encouraging people not to give out their medical information.

Chairman SCOTT. Why don't we finish by each of you just—if you are going to talk to your grandparent, all right, what would you tell them the one takeaway that would reduce their chance of some of that happening?

Ms. CORDERO-STUTZ. I think it is having a trusted relative in the family that they can turn to, to ask before they act. I think that

could be—you know, it could be a grandchild for one family member, or it could be a child or I would say a spouse, but I think in that case, I would like to go another generation. Having someone that you have confidence in. If in fact there is a crisis that needs to be addressed, they should be involved in that process. Urgency should not take over when it comes to being responsible in the actions you are taking, especially with your finances, so that you don't become a victim.

Chairman SCOTT. Yes.

Mr. JOHNSON. Thank you, Chairman. I totally agree and just would add, I think one of the things that is important for not only our grandparents to know, but for us to recognize is that there is an unconditional love and trust that allows somebody to disclose something that could be embarrassing because I think one of the things that—and we have talked about it, and I know you have talked about this in past hearings—that one of the things that we really have to battle is the culture of silence around frauds and scams.

If we make sure that a grandparent who comes to us and says, I lost some money to a scammer, feels supported that they got scammed by a bad person who needs to be pursued and brought to justice rather than, oh, maybe you shouldn't be in control of your finances anymore. That loss of independence is such a fear point for many older adults that they won't have that conversation. We have got to get over that.

Chairman SCOTT. We have been told you have to move out of the house or——

Mr. JOHNSON. Yes, I mean, we—yes, exactly. We have got to be able to help create a culture in which it is okay to say there is something suspicious going on to your trusted family, and I need your help.

Chairman SCOTT. Kathy? I like your idea about the passcode.

Ms. KRANINGER. Yes.

Chairman SCOTT. Yes.

Ms. KRANINGER. It is definitely a key. I mean, having the family password and having the trusted contact is absolutely huge. I will say a good reminder and the prevalence of all of these things is don't engage and don't click, you know? You may actually answer that phone call, which I guess is fine because, you know, you have someone you are expecting to hear from, but the ″don't engage and don't click″ is definitely the—you know, hang up. If you think it is something real, call the number you have. Don't call the number, you know, or don't engage with the person who has called you, and definitely don't click on whatever it is. Again, go to the email address you have. You know, contact the person via that mode is something I would add, but the first two are huge.

Chairman SCOTT. Yes, that is right. They tried to use a—to a family member, they just changed one digit of the email to try to get at somebody to do that.

Ms. KRANINGER. Yes, I mean, it is endless. The last thing, I am getting three a day, and we are trying to figure out how to deal with them because they are coming from my email address, spoof my email address, but it is voicemails.

Chairman SCOTT. Yes.

Ms. KRANINGER. We got a new phone system, and somehow—I don't know how they knew that, but the timing was perfect. We had a new phone system, and now I am getting these voicemails emailed to me, which is a service that exists, but it is not one that we subscribed to.

Chairman SCOTT. Do you think people should answer numbers that are not in their phone?

Ms. KRANINGER. Yes, I mean, I will admit I am guilty of it sometimes, and I am glad I do, because sometimes it is, for example, somebody in your office that I don't know, and it is a 202 number, answer it, but I do think that is that is—for each person, again, if they are expecting or not expecting it, but I will admit I answer those calls, but definitely it is a better idea to let them leave a voicemail or text you before.

Chairman SCOTT. Yes. Brandy, what is one thing that for sure everybody should do?

Ms. BAUER. Read your medical bills and statements, and I am guilty of not doing this myself and working in the Medicare fraud space. I can attest to——

Chairman SCOTT. Your credit card statements——

Ms. BAUER. Yes.

Chairman SCOTT [continuing]. all those bills.

Ms. KRANINGER. Yes.

Ms. BAUER. Revise your statements. I mean, we have heard across the country from your constituents as well. Medicare is a very important program for Americans.

Chairman SCOTT. Right.

Ms. BAUER. We all want it to be here for the future, but in order to ensure that, we need to make sure that we are protecting it on all levels, and so scrutinizing those, reporting anything that is suspicious, it costs you nothing to report it.

Chairman SCOTT. Okay. For each of you, is there anything that Congress or, since we are in Florida, state government should do that we are not doing? Is there anything that you guys think that we ought to be doing that we are not? Let's start with the sheriff.

Ms. CORDERO-STUTZ. Well, I think that having the conversations—I think Jeff mentioned it early on that we here at the local level identify some of those concerns maybe a lot sooner than it gets at the federal level, but having that power come down from the federal level, down is also very helpful. I think maintaining conversations, such as the one we are having today, listening at the local level when it comes to how you are going to legislate in the future, and obviously, help us with the resources. As law enforcement, I am going to advocate for resources support all the time. We need at our local level but——

Chairman SCOTT. And coordination.

Ms. CORDERO-STUTZ. And coordination, absolutely. Thank you.

Mr. JOHNSON. Thank you for asking that question, Mr. Chairman. AARP is a nonpartisan advocacy organization, and, as you know, we always have a laundry list of potential bipartisan bills that could move forward at some point along the way, but I have to say—and both the sheriff and Brandy mentioned this—the Older Americans Act reauthorization is critical. When we talk about the loneliness and isolation that people experience in older adulthood,

OAA, among the many things it does, helps address that, and I appreciate you championing the reauthorization of that.

Chairman SCOTT. I would be shocked if it doesn't happen.

Mr. JOHNSON. Good.

Chairman SCOTT. It is not very functional right now. Do you see that?

Mr. JOHNSON. Yes.

Chairman SCOTT. Other than that——

Mr. JOHNSON. Right. Other than that, exactly.

Ms. KRANINGER. Yes, building on the coordination, Senator, is definitely one of the things that we want to see happen in that information sharing in particular, and that is why we are advocating for that financial crime intelligence center, and there is a lot of work to do on how that looks, you know, in Florida and how it should look. It is going to be different than Texas, but it gives the mechanism to pull up the local information that is unfortunately too scattershot. It is too many, you know, points, and they can't connect until you pull them at the state level, and then you have the opportunity to interact better with the Federal Government with the things that they are seeing, and so it is a good locus in my experience and a lot of the things around fusion centers that have worked.

I think the one thing that the Attorney General's Office is saying is, let's make sure we actually prosecute those crimes then, and that is a huge connection point. I am hopeful that we can do something like that at the state level that is a model and that, you know, with banks and telecommunications companies getting, you know, feeds from that too in terms of actionable information so that is a two-way street, but that is an exciting thing I think that we are looking to really get more, you know, support around.

Chairman SCOTT. Brandy?

Ms. BAUER. As somebody who works in the aging space, I just want to thank you and the bipartisan Senate Aging Committee. Really you have been on the forefront of advocating for older adults for the programs that support them and the Older Americans Act. I think, you know, to echo my colleagues here, the Older Americans Act supports so many things in communities that put eyes and ears on the ground that can help protect people from fraud.

Chairman SCOTT. Well, I want to thank everyone for being here today and participating, and I look forward to continuing to work with community leaders on the frontlines of this important issue to make sure we are empowering and protecting our seniors. I mean, it has impacted every family, I mean, so I can just tell you all the stuff we get all the time. We all get inundated with this stuff, the texts, the emails, the letters, so we all have to get smarter about it.

Thanks, everybody, for being here.

[Whereupon, at 11:07 a.m., the Committee was adjourned.]

APPENDIX

Prepared Witness Statements

U.S. SENATE SPECIAL COMMITTEE ON AGING

"PROTECTING FLORIDA'S SENIORS: FIGHTING FRAUD AND FINANCIAL EXPLOITATION"

AUGUST 7, 2025

PREPARED WITNESS STATEMENTS

Hon. Rosie Cordero-Stutz

Good morning Chairman, distinguished panelists, and everyone present. Welcome to the Miami-Dade Sheriff's office. This is your home. Thank you, Chairman Rick Scott, for your leadership and continued commitment to protecting America's seniors. It's an honor to stand beside you in this critical fight.

Florida is home to one of the largest senior populations in the country, and here in Miami-Dade County, we're proud of the enormous value our older residents bring to our families, our neighborhoods, and our history, but as Chairman Scott has long understood, our seniors also face growing threats from scams, abuse, and financial exploitation. Those threats are only becoming more sophisticated.

Since taking office in January, I made a promise to our residents: to do everything in my power to protect our elderly population from harm. That's why I launched a set of online tools to make it easier for people to report fraud and abuse. I've said it before and I'll say it again-these deceptive schemes can cause life-changing harm, but awareness and prevention can make all the difference.

Chairman Scott's work on the U.S. Senate Special Committee on Aging is a beacon of leadership. His dedication through the TRACED Act (Telephone Robocall Abuse Criminal Enforcement and Deterrence) and pushing for the reauthorization of the Older Americans Act shows his deep understanding that protecting seniors is not just a policy priority, it's a moral responsibility. Chairman Scott has reminded us that more than 10 million Americans benefited from the Older Americans Act program last year. That includes meal delivery, transportation, and day services. Those programs provide much needed support to the elderly. Through visitations, workers can detect signs of abuse or neglect.

At the Miami-Dade Sheriff's Office, our Cyber Crimes Bureau and Economic Crimes Section are working around the clock. From AI-generated scams to cryptocurrency theft and robocalls threatening arrest, these crimes are devastating. Retirement funds are wiped out, victims are saddled with debt, and many are left feeling embarrassed, isolated, and afraid.

Our Cyber Crimes Bureau is staffed with highly trained investigators who are leading the charge working with cryptocurrency exchanges around the globe, including in countries where treaties fall short, to recover stolen funds. We've seen scammers use AI scripts to generate fake websites and realistic investment dashboards. They prey on our seniors through messaging apps, removing human interaction and making detection harder.

That's why timeliness matters. The faster scams are reported, the better our chances of stopping them before they vanish and reappear under a new name.

We will continue to strengthen interagency collaboration. That means stronger ties with federal partners like the FBI, Homeland Security Investigations, and the Department of Business and Professional Regulation.

We must not forget the growing threat of Condo and HOA fraud occurring right here in our backyard, a quiet crisis disproportionately affecting our elderly homeowners. One of my first actions as Sheriff was to set up a hotline, and an email address, for people to call if they suspect public or HOA corruption. Elderly residents are particularly vulnerable to fraud schemes involving unauthorized assessments, embezzlement, or falsified records. These crimes often go unreported or under-investigated due to the complexity of association governance and legal frameworks.

We're working with state regulators to detect fraud in these associations and protect the rights of vulnerable residents. Preventing fraud begins with education, as many homeowners are unaware of their rights. We have a public outreach initiative to empower residents and will continue to do so.

To our residents: don't share your Social Security number or banking info over the phone. Hang up on suspicious callers. The level of sophistication with regard to such scams is increasing. If you get a call from a relative or friend and they tell you to send them money immediately, verify it by calling them back on a trusted number. Never let urgency override common sense.

To our agencies and partners: let's keep pushing. Let's coordinate more, train more, and share more. Because in a perfect world, every senior in our community should live safe, supported, and scam-free.

Thank you and thank you again, Chairman Scott, for standing with us in this mission.

U.S. SENATE SPECIAL COMMITTEE ON AGING

"PROTECTING FLORIDA'S SENIORS: FIGHTING FRAUD AND FINANCIAL EXPLOITATION"

AUGUST 7, 2025

PREPARED WITNESS STATEMENTS

Jeff Johnson

Chairman Scott thank you for inviting AARP to testify today. My name is Jeff Johnson, and I am the State Director for AARP Florida. AARP advocates for the more than 100 million Americans age 50 and older, including 10 million Floridians.

AARP is very grateful to the Committee for their work examining the growing threat of scams and financial fraud targeting older Americans and exploring community, state, and federal strategies to prevent exploitation. This Congress, the Committee has held a number of important hearings, including one last week on Combating Elder Abuse & Neglect. We are very grateful for your efforts to highlight the issues that matter most to older Americans. We also appreciate the Committee's work to spotlight financial literacy and fraud prevention efforts, including the Committee's 2025 Fraud Report and the Chairman's Financial Literacy Report.

Thank you for the opportunity to provide testimony at today's hearing about preventing scams and strengthening financial security - which is at the heart of who we are and what we do at AARP. AARP has long worked to educate consumers, support financial exploitation victims, and improve financial exploitation detection and prevention across industries, and we look forward to continuing to work with you towards policy solutions to prevent exploitation and protect victims.

Fraud in America is at crisis levels. The Federal Bureau of Investigation's (FBI) numbers show a dramatic increase from the $800 million in fraud losses in 2014, to 2024, when hardworking Americans had $16.6 billion stolen from them. This is almost a 2000 percent increase in fraud losses over the past decade. Floridians reported the theft of over $1 billion from fraud in 2024 - over a third of which (nearly $400 million) was stolen from adults aged 60 and older, and that is likely a very low estimate. In a 2024 report, the FTC estimated the true overall 2023 fraud losses, adjusted for underreporting, was $158.3 billion for consumers of all ages and $61.5 billion for older adults.

Transnational organized crime groups are operating openly abroad, siphoning hard-earned money out of our local communities and economies. This is money that older adults had saved for their retirement - to spend on their hobbies, on travel, on their grandchildren - and instead it is lining the pockets of criminals abroad, and because of vast under-reporting, this is likely a small percentage of actual losses. An AARP study in 2021 estimated 9 in 10 Americans encountered a fraud attempt, and 1 in 7 had money stolen from them in 2020 alone. Given the significant and steady increase we've seen in fraud year after year, we can extrapolate that even more Americans are likely to report losing money to scams now in 2025.

According to FBI data, older adults reported higher losses than younger adults in 2024, with an average loss of $83,000 for those age 60-plus reporting a fraud loss, compared to $19,000 for all ages. Older adults are often targeted by criminals because they have more money - they have had a longer time to accumulate savings and are therefore appealing targets for criminals. These losses can have significant impacts on the financial security of older Americans, as they are often living on fixed incomes and can scarcely afford to lose funds to criminals, and older Americans aren't just losing their retirement savings from fraud - in some cases they're even losing their homes.

Just last month, AARP's Fraud Watch Network Helpline received a report from Edward[1], a Florida man in his sixties who had the entire proceeds from the sale of his home stolen by cybercriminals - more than $400,000 in total. Scammers were able to access and drain the man's bank account before he was able to secure new housing. With all his money gone, this older Floridian went from cashing in on his primary investment (his home) and securing affordable housing to facing the threat of homelessness in a matter of seconds.

Victims come from diverse backgrounds - criminals do not discriminate when it comes to targeting potential victims. AARP's Fraud Watch Helpline has made clear to us that fraud happens to everyone - it does not matter a victims' age, their in-

[1]1A **Victim names have been changed for privacy reasons.

come level, where they live, or what level of education they have. Everyone is susceptible to fraud.

For many fraud victims, the financial toll is only part of the story; research shows nearly 2 in 3 victims suffer a significant health or emotional impact. This is only worsened by the stigma and victim-blaming associated with fraud. While our society treats many victims of other crimes with compassion, we tend to place responsibility on the victims of fraud who ″fell for″ a scam - blaming victims for not being smart enough or paying close enough attention in the first place.

The reality is that the criminals who carry out these scams have professionalized their industry - they are experts at convincing people to send them money via a plethora of different and constantly evolving scams. Given the increasingly sophisticated nature of scams through the use of advanced technologies it is unsurprising that these criminals are also becoming increasingly successful in committing fraud.

Not only does victim-blaming and the stigma associated with fraud have a profound and devastating impact on victims, it also discourages victims from reporting fraud, which prevents us from identifying the true scope of this crisis. It is vital that we change the narrative on fraud victimization. AARP has conducted extensive research and developed resources to help educate professionals on the importance of the language we use when working with victims. For example, when we say, ″criminals stole [the victim's] money″ instead of describing the victim as having ″lost money to a fraudster,″ clearly places the responsibility of the crime where it should be - on the criminal, not the victim.

Addressing fraud prevention is a top priority for AARP and has been for many years. In my testimony, I would like to share some of the initiatives that AARP has worked on in this space, including the Fraud Watch Network Helpline, as well as to describe the work we have done here in Florida by educating consumers about fraud and scams, as well as advocating for resources and policies that support victims of fraud and assist law enforcement with investigating and prosecuting perpetrators.

AARP's Fraud Prevention Work

While this fraud awareness and prevention has always been a priority for AARP, our fraud prevention work has grown over time as we have increasingly heard from our members that fraud is a top concern for them and their financial security. The AARP Fraud Watch Network was created in 2013, and our fraud prevention work through our state offices has grown significantly in recent years, including here in Florida.

AARP works with victims of fraud through our Fraud Watch Network, which offers resources to arm consumers with the knowledge needed to spot and avoid scams. The Fraud Watch Network Helpline is a free resource available to people of any age; you do not have to be an AARP member to use the service. In 2024, the AARP Fraud Watch Network Helpline fielded over 100,000 calls from concerned Americans reporting attempted frauds and scams, as well as those recounting their traumatic experiences of fraud victimization, and the theft of their personal information and/or finances.

For example, just law month, Roger, an 85-year-old Floridian, called the Helpline to share his experience. Roger had over $150,000 stolen from him in a tech support scam. A criminal called him, posing as Apple, and told him the only way ″to protect″ his money from hackers was to convert and send his money in gold. Another Floridian, Carlos, who is in his 70s, was defrauded by a friend he made in his senior exercise class. This ″friend″ appears to be part of a network that stole more than $650,000 from the man. Unfortunately, there are many more stories just like these. In June of this year, the Helpline received multiple reports from seniors who had formed friendships and romances online with criminals who stole over $100,000 in each case. These are just a few of the many, many devastating stories our Fraud Watch Network Helpline staff and volunteers hear from Floridians every year.

AARP provides extensive community outreach through the Fraud Watch Network and our 53 AARP state offices. We hold events in communities to raise awareness about different types of fraud and scams. We also partner with law enforcement, regulatory agencies, and Attorneys General to host webinars, tele-townhalls, trainings, and other fraud prevention and awareness events. We have more than 800 volunteers nationwide who deliver fraud education in their communities and work directly with victims of fraud. Each year we reach hundreds of thousands of AARP members and non-members alike from coast to coast with our locally driven outreach efforts.

AARP has a Fraud Resource Center and writes extensively about fraud in the AARP Magazine and AARP Bulletin. Articles and resources include recent fraud news, information about common scams, trends in fraud, and how to recognize and avoid common scams, as well as resources to assist victims of fraud and their fami-

lies when they encounter scams. We also have videos that break down how scams work and how to keep yourself safe from criminals. Recent articles have included, ″3 Key Things to Know About Scams in 2025″ and ″I Never Thought My Dad Would Become a Romance Scam Victim. Don't Make My Mistake″ and ″SIM Swapping: Scammers Hijack Smartphones and Steal Thousands″. These publications reach millions of Americans and fraud-related articles are some of our most-read and well-received - an indication of how worried our members are about fraud.

AARP launched a weekly podcast called The Perfect Scam in 2019 to highlight the different types of fraud and scams that we were hearing about from our members and callers to the Fraud Watch Network Helpline. Our host introduces listeners to those who have experienced scams firsthand, as well as leading experts who pull back the curtain on how scammers operate. In December 2023, the New York Times highlighted the scam podcast as a top resource to ″deepen your understanding of how liars and con artists operate.″ Recent episodes have focused on credit card scams, rental scams, gold bar scams, pet scams, charity scams, time share scams, arrest warrant scams, military benefit scams, romance scams, and job posting scams, among many others. Most of these stories come directly from victims we have worked with on the Helpline who want to share their story to help others avoid similar experiences.

The AARP Fraud Watch Network has also developed a free program to provide emotional support to fraud victims and their friends and relatives. AARP's Fraud Victim Support Group provides individuals with an online forum to meet and interact with others who have experienced similar events. Our sessions are a safe environment to give and receive valuable feedback and support from others who are on the road to emotional healing and recovery. Group sessions are confidential and led by trained facilitators who offer fraud education and understanding to participants, as well as time for meaningful peer-to-peer sharing and support. Participants don't have to be the primary victim of a fraud to participate- family members, partners or friends of a fraud victim are welcome and encouraged to participate. Experiencing fraud can be devastating, and these types of safe spaces can be very valuable to victims and their loved ones in processing and recovering from the trauma it causes.

AARP also runs a program called BankSafe, which trains employees at financial institutions to detect fraud and financial exploitation. BankSafe works with the financial services industry to help them stop financial exploitation before the money leaves customers' accounts. The program encourages those in the financial services industry to voluntarily adopt research-proven interventions, policies, and procedures that effectively prevent exploitation. Researchers from the Virginia Tech Center for Gerontology have studied the impact of training bank and credit union staff to spot and prevent financial exploitation. In 2018, a Virginia Tech study with over 2,000 frontline employees in 11 states (including Minnesota and Vermont) found that employees who took the BankSafe training saved 16 times more money than those without the training. Based on these findings, we estimate that BankSafe policies, interventions, and procedures have, to date, prevented more than $450 million from being stolen from consumers.

In addition to our fraud prevention awareness, industry collaboration, and victim support services, AARP conducts research on fraud to inform our work and the public at large. According to a 2025 AARP survey on the Fraud Crisis in America that surveyed American adults (those 18 and older), adults of all ages worry greatly about fraud (37 percent), but this fear is even more pronounced among adults ages 50+ (44 percent). The survey also demonstrated that people continue certain behaviors that put them at a higher risk of becoming the victim of fraud. For example, while most adults reported that they rarely or never answer unknown phone calls, texts, or friend requests, over a third of adults (36%) reported that they usually or always answer one or more of these unknown communications. The survey also looked at how adults were maintaining the security of their devices and online accounts, including the use of VPNs and two-factor authentication, downloading free apps and/or taking online quizzes on social media, and using different passwords on all accounts.

AARP's comprehensive approach to fraud prevention-spanning education, advocacy, direct support, and industry collaboration-demonstrates our steadfast commitment to safeguarding the financial well-being and peace of mind of older Americans. Through continued community engagement, we can work to ensure that everyone is equipped to recognize, resist, and recover from scams-protecting not only personal assets, but also restoring trust and security across our communities.

AARP's Work to Educate Florida Consumers About Fraud

Here in Florida, AARP is also investing in educating consumers about the scams and frauds we're seeing across the state, as well as providing Floridians with the easy-to-access resources they need to report and respond to fraud when it occurs.

We've created a unique online Florida Fraud Resource Center (AARP.org/FLFraud) that acts as a one-stop shop for Florida-specific fraud resources, providing consumers with comprehensive guidance on how and where to report fraud and exploitation at the local, state, and federal levels - information that can take hours to research when you don't know where to start.

Another resource you'll find through our virtual fraud resource center is a digital library of free, easy to download and print one-pagers on the scams that are most frequently impacting Floridians - which, once again, provides consumers with clear guidance on how and where to report the many different types of fraud in Florida. These resources were created by AARP's Florida fraud prevention team with Florida law enforcement in mind - drafted with suggestions and input from law enforcement partners like the Florida Sheriff's Association, then promoted and shared with law enforcement across the state for broad use and dissemination in their communities and on the front lines.

We're working closely with state and local law enforcement partners to increase Floridians' awareness and utilization of some of the great fraud prevention resources currently being offered by these agencies, as well as to encourage the adoption of best practices and implementation of similar programs by law enforcement agencies statewide. For example, our team recently showcased the SafetyNet program of the Walton County Sherriff's Office, which offers isolated residents in the Florida Panhandle with a life-line - social connection through the sheriff's office that provides meaningful health and safety protections, while reducing residents' risk for potentially devastating cases of fraud and exploitation too often caused and/or concealed by social isolation.

AARP also works to educate older Americans about fraud and scams through our network of state volunteers and staff across the country, especially here in Florida. We host practical fraud prevention events in communities across the state, including shred events that allow residents to safely dispose of sensitive information that might otherwise fall into the hands of fraudsters. Often, these events are paired with educational seminars and trainings, which are sometimes led by AARP Florida volunteers or held in conjunction with fraud prevention experts and professionals. Within the past year, AARP hosted two different Fraud Prevention Summits in partnership with the U.S. Department of Justice here in Florida - one in The Villages, a retirement community spanning across three counties in Central Florida, which boasts a median population age of 73.6, and one in another major 55-plus community in Southeast Florida.

AARP also recognizes the needs and availability of older adults are varied, and our membership includes full-time working professionals and family caregivers who may be unable to attend an in-person event. This is why AARP leverages technology to keep Floridians educated on the latest scams through the use of virtual webinars and teletown halls, expanding educational opportunities and making fraud education accessible for everyone. We've also embraced and harnessed the wide appeal of AARP's social media channels to regularly promote fraud prevention messaging, like through our Fraud Focus Friday posts here in Florida, which we utilize to share key fraud prevention tips and resources.

AARP's State-Level Fraud Prevention Advocacy Work

AARP works actively across the states - including here in Florida - to protect consumers-especially older Americans-from fraud and scams. Through advocacy and collaboration, AARP has supported state laws and regulations tackling real estate scams, cryptocurrency kiosk fraud, suspicious financial transactions, and gift card fraud, providing model policies and practical protections that strengthen safeguards for consumers at the state level.

Preventing real estate scams

Thirty states enacted legislation against the predatory practice of unscrupulous real estate brokers who misled homeowners into signing decades-long agreements that gave the brokers the exclusive right to sell the homes. The bills enacted in these states are based on a model bill designed by AARP and other national stakeholders. It prohibits service agreements of more than one year, makes the agreements nonrecordable in the deed or property record, and blocks liens or encumbrances associated with the land. It also prohibits locking homeowners into exclusive long-term real estate listing agreements and imposes penalties on brokers who do so. (Learn more on this episode of AARP's The Perfect Scam podcast.)

I'm proud to say that Florida was among the first states to combat this issue through both the timely enactment of state legislation and the civil enforcement sought by former Florida Attorney General and current U.S. Senator Ashley Moody against these predatory businesses.

Preventing cryptocurrency kiosk scams

AARP is advocating across the country for important consumer protections that will deter criminals from leveraging cryptocurrency kiosks, also referred to as Bitcoin ATMs, in their schemes. AARP's Fraud Watch Network has seen a dramatic increase in the number of fraud victims being directed to send funds via cryptocurrency kiosks. Providing essential consumer protection standards for cryptocurrency kiosks will prevent older Americans from losing their hard-earned money to criminals. Minimum standards include requiring money transmitter licensing of cryptocurrency kiosk operators in the state, implementing daily transaction limits to reduce fraud dollar losses to the criminals exploiting these cryptocurrency kiosks, and mandating refunds to victims of the fraud facilitated by these machines. Here in Florida, our state legislature has considered legislation that would offer some oversight and protection for Floridians with regard to the nearly 3,000 cryptocurrency kiosks currently operating across the state -first in 2024 with House Bill 977 and Senate Bill 662 (Virtual Currency Kiosk), and earlier this year with House Bill 319 and Senate Bill 292 (Virtual Currency Kiosk). While these bills have not yet crossed the finish line in the Florida Legislature, it has been encouraging to see Florida city and county governments step into the gap. Several local governments are considering locally regulating these machines to protect their residents, often at the urging of law enforcement leaders in those communities.

Enabling financial institutions to hold suspicious transactions

One of the most pressing challenges across the states is the lack of clear, consistent guidance around the reporting and holding of suspicious transactions. ″Report and hold″ laws allow financial institutions to delay or refuse transactions when they suspect financial exploitation, giving time to intervene before money is irreversibly lost. Research from Virginia Tech has shown that even brief delays can significantly reduce harm, especially when the victim is already in a heightened ″fight-or-flight″ state and may not be capable of rational decision-making. However, while these laws are effective, especially when used by broker-dealers who are federally permitted to act under them, a regulatory gap remains. Banks and credit unions, primary depository institutions, are generally barred from using these tools unless their individual states have explicitly passed laws allowing it. This is due in part to the limitations imposed by federal Regulation CC (enacted in 1989), which governs funds availability and does not provide carve-outs for suspected fraud. As a result, the institutions best positioned to stop real-time exploitation often lack the legal authority to do so, despite clear evidence that the intervention works. In a recent report from the American Bankers Association, nearly 90% of banks located in states that do not have the power to hold suspicious transactions would find it helpful to have that ability.

AARP has worked on model state legislation to enable securities and investment firms to hold transactions that are suspected to be related to fraud and financial exploitation for a short period of time while there is an investigation (″report and hold″ laws). Almost all states have passed this or a similar law, and roughly half of the states have also applied this model to banks and credit unions. Congress could consider a federal law to enable financial institutions to hold suspicious transactions while they investigate them further. In 2024, here in Florida, AARP worked with stakeholders like the Florida Bankers Association to pass Senate Bill 556 (Protection of Specified Adults), which now authorizes Florida banks and credit unions to temporarily delay transactions reasonably believed to involve the exploitation of older and vulnerable Floridians under specified conditions.

Preventing gift card fraudWith AARP's help, ten states this year have enacted legislation advancing legislation aimed at curbing gift card fraud. Criminals use gift cards in their fraudulent activity through collecting the information directly from the victim or tampering with the card so they can steal its value. To help curtail gift card scams, AARP's state offices have helped pass comprehensive legislation requiring stores where gift cards are sold to post a notice alerting customers to protect themselves from gift card scams and what to do if they are the victims of this scam, staff training, secure packaging, and record keeping. This year, AARP had the opportunity to support Senate Bill 1198 (Fraudulent Use of Gift Cards) here in Florida, which provides much needed clarity to law enforcement and prosecutors on charging criminals in cases involving fraud or theft through gift cards, as well as enhanced penalties for criminals with prior related convictions.

Innovative elder justice work

AARP recognizes that all forms of elder abuse, including financial exploitation and fraud, are often hidden and challenging to detect or identify, which is why AARP supports policies that aid in the earlier detection of, and intervention in, elder abuse cases. Here in Florida, AARP had the opportunity to support two innovative elder justice-focused bills that I'd like to highlight.

In 2018, AARP supported legislation introduced by elder justice stakeholders creating a first of its kind injunction for protection against the exploitation of vulnerable adults in Florida (House Bill 1059). This unique resource was inspired by and modeled after similar long-standing resources available to victims of domestic violence in Florida. Since the creation of this exploitation injunction resource in 2018, AARP has continued working with stakeholders to expand and improve this injunction resource as to its application and capabilities in combatting elder fraud and exploitation - amending and improving Florida Statute ⧫ 825.1035 in 2021, 2023, 2024, and again this year. Thanks to the most recent legislation in 2025 (Senate Bill 106), Florida qualifying victims of financial exploitation and fraud can now avail themselves of the protections offered by the exploitation injunction process in cases where the perpetrator attempts to conceal his or her identity and whereabouts by using social media, messaging applications, email, or phone calls and texts to carry out the crime.

AARP's recent elder abuse advocacy efforts also extend to our work on House Bill 1540 in 2023, where we advocated alongside law enforcement and prosecution partners from Florida's Fourth Judicial Circuit to protect and preserve the important work of the first-ever elder abuse fatality review team in the state. We recognized the critical need for elder abuse fatality review teams in cases of abuse, neglect, and exploitation resulting in the death of vulnerable adults in Florida, as well as the significance of findings and recommendations from teams like these in crafting meaningful elder abuse policies and resources at the local, state, and federal levels.

AARP's Federal Fraud Prevention Advocacy Work

AARP has also endorsed a number of pieces of federal legislation in the fraud prevention space. These bills aim to strengthen protections for consumers, especially older Americans, against various forms of fraud and financial exploitation. They propose measures such as providing resources to law enforcement, giving victims tax relief, increasing transparency in communications, enhancing oversight of financial products and services, and raising public awareness about scams and identity theft. Collectively, the legislation would empower agencies and consumers, close regulatory gaps, and implement new safeguards to help prevent criminals from targeting vulnerable individuals.

* AARP endorsed S. 2544/H.R. 2978, the GUARD Act, which Chairman Scott has championed. This bipartisan legislation would provide state and local law enforcement with federal grants to allow them to hire and train staff and secure specialized software and other tools to improve their capacity to conduct fraud investigations. This will ensure law enforcement has the tools they need to lock up the criminals who victimize older Americans.

* AARP endorsed S.1773/H.R.3429, the Tax Relief for Victims of Crimes, Scams, and Disasters Act. This legislation would reinstate the casualty and theft loss deduction, better ensuring fraud victims don't have to pay taxes on stolen funds. Currently, if you have money stolen from retirement or other taxable accounts, the IRS may tax you on money you already lost to criminals. This legislation will help end the injustice currently written into the tax code by allowing victims to deduct the amounts stolen from them on their taxes.

* AARP endorsed H.R. 1027, the Quashing Unwanted and Interruptive Electronic Telecommunications (QUIET) Act. The QUIET Act mandates transparency from robocallers, requiring them to disclose upfront when artificial intelligence is used to imitate human voices in calls or text messages. Additionally, the legislation doubles financial penalties for those who use AI to impersonate individuals, commit fraud, or obtain valuables under false pretenses.

* AARP endorsed H.R. 1469, the Senior Security Act of 2025, which would help combat financial exploitation by creating an interdivisional task force at the Securities and Exchange Commission to examine and identify challenges that older people face while investing. The bill would also require the Government Accountability Office to study and report on the economic costs of the financial abuse of older Americans.

* AARP endorsed S.1699, the Artificial Intelligence Public Awareness and Education Campaign Act, which would launch a comprehensive public awareness, education, and consumer literacy campaign to educate consumers about the prevalence of AI in their daily lives. Empowering older Americans with this information will not only help protect against fraud and abuse but also inform them of AI's positive potential to assist with daily tasks.

* AARP endorsed S.1666, the Improving Social Security's Service to Victims of Identity Theft Act. This legislation would streamline and improve the assistance provided by the Social Security Administration to individuals whose Social Security number has been stolen or misused. Identity theft and fraud are at an all-time high

in the United States, and the range of fraud that can be committed with a stolen Social Security number is truly staggering.

* AARP endorsed S.2019, the Taskforce for Recognizing and Averting Payment Scams Act (TRAPS Act), which aims to protect older Americans from financial scams. This legislation would create a task force to combat digital payment scams. The task force - composed of financial regulators, institutions, and consumer advocates - would analyze fraud trends and develop strategies to enhance protections.

* AARP endorsed H.R.1734/S.2117 the Preventing Deep Fake Scams Act. This bipartisan legislation will establish a dedicated task force on AI in financial services that would include representatives from key financial services regulatory agencies, financial institutions, third-party vendors, and AI experts to explore the use of AI in the financial sector to commit and detect fraud.

* AARP endorsedH.R.40*R.2808/S.1467, the Homebuyers Privacy Protection Act. This bipartisan legislation takes important steps to protect older Americans - who make up more than 75 percent of U.S. homeowners - from misleading and fraudulent solicitations during home transactions. By requiring consumers to opt in before their credit inquiry data can be sold and limiting the use of mortgage ″trigger leads,″ the bill helps prevent scams that exploit major life events like buying or selling a home.

* AARP endorsed H.R. 40*R.306, the Ending Scam Credit Repair Act, or ″ESCRA.″ This bill would address issues in the credit repair industry. Credit repair organizations (CROs) often exploit customers by falsely promising that they can repair a consumer's credit score. ESCRA would introduce new rules to shield consumers from misleading and fraudulent practices.

Conclusion

Addressing fraud requires more than piecemeal solutions; it demands a whole-of-society approach. We cannot educate our way out of the fraud crisis. Industry cannot mitigate and engineer our way out of it. Policymakers cannot regulate our way out of it, and law enforcement cannot arrest our way out of it, but, together, educators, policymakers, law enforcement and industry can turn the tide against the vicious criminals who hold the power right now. Together, we can disrupt their business model, protect millions of consumers, and safeguard billions of dollars in savings and retirement accounts and in our economy.

I am proud to say that, even though there is much work to do, Florida is an example of what this type of comprehensive approach could look like. AARP Florida is working directly and through diverse partnerships to provide real-time education and support to our neighbors who are at risk of being scammed. We also are working with policymakers at all levels of government to improve laws and regulations to protect consumers and prosecute fraudsters, and we work with law enforcement agencies across the state that have identified the dramatic scope and impact of senior fraud on their communities and are striving to fight back. There is much more work to do, but we all recognize the importance of this issue, which is the first step toward turning the tide.

We thank Chairman Scott and the Committee for bringing attention to this important issue and look forward to working with you to turn the tide on criminals committing fraud.

U.S. SENATE SPECIAL COMMITTEE ON AGING

"PROTECTING FLORIDA'S SENIORS: FIGHTING FRAUD AND FINANCIAL EXPLOITATION"

AUGUST 7, 2025

PREPARED WITNESS STATEMENTS

Hon. Kathy Kraninger

Introduction

Chairman Scott, on behalf of the Florida Bankers Association (FBA) and our more than 150 member banks operating in the great state of Florida, I am honored to appear before you on such a crucial topic. Banks are on the front line of the fight against fraud, working to protect our customers from scams, identity theft, and cybercrime. Fraud has become more complex and more prevalent, impacting individuals, families, businesses, and communities across Florida and the nation.

While some of the most troubling cases affect the most vulnerable among us such as older Americans who are the focus of this Committee, no one is immune from the barrage of attempts via every mode of communication in our modern society. It is a game of numbers - the sheer volume and ease of attempts means more success for the bad guys.

The FBA advocates for a national strategy that will tackle fraud and scams from all angles, including cutting off communication channels to targeted victims, bolstering public education, and ensuring prosecution of criminals. We are committed to strengthening collaboration among financial institutions, telecoms, tech companies, law enforcement, and policymakers, as well as engaging the public, to combat fraud, enhance consumer protections, and ensure criminals are held accountable.

The FBA works closely with the American Bankers Association (ABA) and the Independent Community Bankers Association, both of which offer services to banks to prevent, identify, and report fraud as well as advocate for initiatives to counter fraud and scams.

Defining the Problem: Fraud and Scams are a Pervasive Threat

Fraud is a national crisis, as documented by this Committee's annual fraud report. In 2024, the FBI's Internet Crime Complaint Center (IC3) received 859,532 complaints, with potential losses exceeding $16.6 billion. This represents a 2% decrease in complaints and a 25% increase in losses compared to 2023.[1]

Meanwhile, the Federal Trade Commission, received fraud reports from 2.6 million consumers last year, similar to 2023, but the percentage of people who reported losing money jumped from 27% to 38% in that same one-year period. The most commonly reported scam category was imposter scams. Losses to government imposter scams in particular increased $171 million from 2023 to a total of $789 million in 2024.

For the second consecutive year, email was the most common way that consumers reported being contacted by scammers. Phone calls were the second most commonly reported contact method for fraud in 2024, followed by text messages.[2] Fraudsters are targeting consumers through increasingly sophisticated channels, including phishing emails, robocalls, social media impersonation, and peer-to-peer payment fraud.

Furthermore, as AI and other technological advancements evolve, scams will only become more convincing and harder to identify for the average American, much less the most vulnerable among us. Older Americans are especially vulnerable-and Florida, with one of the largest senior populations in the country, is disproportionately affected. The losses reported by victims age 60+ went from $3.4 billion in 2023 to $4.8 billion in 2024 according to the IC3.

From inception, a significant number of cyber scams originate from other countries, especially from China and Southeast Asia, as found by the Center for Strategic and International Studies.[3] The analysis documents how the Covid-19 pandemic's lockdowns and strict border controls drove criminal groups to seek new sources of profit. In particular, Chinese criminal groups built cyber-scamming com-

---

[1] https://www.ic3.gov/AnnualReport/Reports/2024—IC3Report.pdf

[2] https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024

[3] https://www.csis.org/analysis/cyber-scamming-goes-global-unveiling-southeast-asias-high-tech-fraud-factories

pounds where human trafficking victims, working under threat to their lives, are coerced to befriend and entice innocent Americans into fraudulent investment schemes.

Financial institutions are often the last line of defense in detecting suspicious activity and preventing significant loss. Our industry is heavily investing in such capabilities, yet it can be incredibly challenging for bank employees to convince customers that the activity is suspicious.

The stories are heartbreaking as they unfold in an all-too-familiar way. The below scam typologies are the most frequently seen by one of our larger institutions serving Florida. Furthermore, from this same institution's reporting, one out of every six elder financial exploitation scams they identify occurs in Florida.

1. Romance scams where the victim/client sends money to the perpetrator: The perpetrator insinuates themselves into the victim's life over time. The perpetrator exploits the victim/client's loneliness and provides constant communication and attention. These scammers can operate ″in real life″ but also purely online. With the aid of technology, this does not require much effort on the perpetrator's part. Even where the client/victim feels used or silly, they fear losing companionship so they send money. For the bank, it is more often than not impossible to overcome that emotional attachment.

2. Confidence investment scams where a victim/client sends increasing amounts into a phony cryptocurrency platform: The victim/client believes they are engaging with a legitimate opportunity because they ″created″ an account and can ″see″ they are making lucrative returns on their investment. How the victim/client is reeled into the scam could also involve a romantic element, which adds all the challenges noted in the first typology. Institutions can have success in overcoming this scam by getting the victim/client to perform their own research on what this scam entails and convincing them to try to withdraw their investment. This scam involves substantial losses because the withdrawal is often not possible, and then the scammer disappears.

3. Impersonation scams where bad actors pose as legitimate companies - often financial institutions - and assert the victim/client's money is not safe: The perpetrator preys on the victim/client's fear that they have already been scammed. The perpetrator will have details about the victim/client that bolster legitimacy (where you bank, what kind of car you drive, etc.). The bad actor directs the victim/client to either wire, transfer or withdraw funds to deposit into a bitcoin kiosk. Clients don't realize they were scammed until after they have sent or withdrawn money.

With respect to funds transfer and means of payment, there is not one particular method that perpetrators particularly exploit. Scammers tell the victims what to do, and victims follow that direction. Funds acquired through these scams can be transferred as cash in shoe box to a Target parking lot; by wire; by cashier's check; via gift cards purchased by the victim; via credit card payment; or when a victim sets up a digital wallet, purchases crypto, and transfers it. While different means of payment and transfer involve different opportunities for intervention, the point of payment cannot be the only opportunity. Efforts to stop these scams should start much earlier than the point of payment, rather they should start at the first communication point.

Engaging all Stakeholders in the Fight

A national strategy that attacks fraud from all angles and stakeholders is key. Where the U.S. problem continues to grow, we can take lessons from what other countries have done. Take Australia, for one example, where the government has seen a 25% decrease in losses reported and 18% decrease in scams reported in the past year, a decline that builds on the prior year's decline.[4] How did they do it?

Collaboration among financial institutions, telecoms, tech companies, law enforcement, and policymakers, as well as engaging the public, to combat fraud and scams is key. Starting with the first outreach to potential victims, telecommunications, technology, and social media companies can play a pivotal role by blocking scam communications before they reach consumers. Australia provides one example of how that could work. The government ingests reported information, investigates and sends out authoritative information that allows banks, social media, and telecoms to safely and efficiently act. In 2024, Australia's National Anti-Scam Centre referred more than 6,000 non-investment scam URLs for assessment and takedown, with 92.0% of those subsequently removed.

While it is mandated in some countries, the U.S. solution could look different. Companies could offer a ″Do Not Contact″ service enabling customers to opt out of calls, texts, and messages from overseas, as an example. The banking industry has

[4] https://www.nasc.gov.au/reports-and-publications/targeting-scams

urged the Federal Communications Commission (FCC) to develop a database of scam messages - i.e., the text messages that consumers report through the ″report junk″ feature on the iPhone and similar feature on Android devices. This database would be accessible to banks, law enforcement, and other legitimate companies, so that these companies can identify ongoing scams targeting the company's customers and take action to mitigate the impact.[5] The banking industry also has been a leading proponent of other FCC proposals to combat fraud perpetrated over our telecommunications systems, including the latest FCC proposal to require caller ID authentication solutions on non-Internet Protocol (IP) networks - i.e., providers of networks that do not rely on the IP for communication.[6]

The banking industry has invested significant resources in tools to identify and stop fraud early. These tools are necessary to support compliance with Bank Secrecy Act (BSA), anti-money laundering, countering terrorist financing, and cybersecurity responsibilities, as well as voluntary efforts to support our customers and protect our businesses. As a few examples, banks:

•Implement rigorous, risk-based BSA compliance and antifraud programs to flag when customers have started to send money in unusual patterns, including to high-risk individuals, entities, and jurisdictions.

•Submit Suspicious Activity Reports (SARs) to the Financial Crimes Enforcement Network (FinCEN) and subscribe to FinCEN's alert on fraud schemes, which offers tips for filing SARs.

•Deny institutions of primary money laundering concern access to the U.S. financial system, such as the Cambodian money laundering Huione Group, in response to section 311 actions by FinCEN.

•Ensure bank employees are trained to identify and report suspicious activity and know what actions to take to protect customers.

•Use the Treasury Department's Treasury Check Verification System to catch canceled, duplicate, or other problematic Treasury checks at the time of presentment.

•Employ National Automated Clearing House Association's (Nacha) rules intended to reduce the incidence of frauds, such as business email compromise, that make use of credit-push payments, as well as support the ACH Contact Registry.

•Utilize the ABA Check Fraud Claim Directory that maintains contact information for banks needing to file a check warranty breach claim with another financial institution.

•Deploy additional tools like real-time fraud detection analytics, voice biometrics, and identity verification platforms that are proving effective in detecting anomalous behavior and preventing fraud before money is lost.

Where permitted by law and protected from liability, banks can delay certain transactions when they suspect financial exploitation of an older or vulnerable person. In 2024, here in Florida, FBA worked with AARP to pass Senate Bill 556 (Protection of Specified Adults)[7], which authorizes Florida banks and credit unions to temporarily delay transactions reasonably believed to involve the exploitation of older and vulnerable Floridians under specified conditions. More than half (54.5%) of bank respondents in states with these ″hold″ laws have used them to prevent elder financial exploitation, according to a recent ABA Foundation survey.[8] Delays are helpful in bringing a family member into the conversation or giving the client the opportunity to stop and think. However, where the client/victim wants to proceed with a transaction with their money, the financial institution ultimately has to do what the client asks.

In 2025, the FBA worked alongside AARP and others to pass SB 106[9] to permit substitute service of process in an injunction proceeding to protect vulnerable adults against financial exploitation by an ″unascertainable″ perpetrator who has communicated with the vulnerable adult victim by untraceable means, such as a text message or phone call. The substituted service must be made by the same manner of communication that the perpetrator used to contact the vulnerable adult victim. Upon issuance of a final injunction by the court after substituted service has been used, a 30-day freeze on any proposed transfer of funds or property is initiated.

That is why consumer education is essential to prevention of harm. Banks have invested in campaigns like the ABA's ″Banks Never Ask That″ and ″Practice Safe

---

[5] https://bankingjournal.aba.com/2024/11/stick-it-to-the-scammers.

[6] https://www.aba.com/advocacy/policy-analysis/ABA-Urges-FCC-to-Impose-Call-Authentication-Requirement-for-NonIP-Networks.

[7] https://laws.flrules.org/2024/200

[8] https://www.aba.com/news-research/analysis-guides/state-hold-laws-and-elder-financial-exploitation-survey-report

[9] https://laws.flrules.org/2025/158

Checks″ initiatives. We partner with organizations like the AARP and bank regulators highlighting their messaging and campaigns. We encourage older Americans to include trusted contacts on their financial accounts so we can contact those individuals to flag suspicious activity or to intervene where a customer is being manipulated by a scammer. We host fraud prevention roundtables and events at our branches and offices, senior centers, libraries, and town halls. Talking about these issues is important as so many victims are embarrassed leading to what experts agree is underreporting of scams and losses. In fact, the FTC reported in 2024 that the estimated 2023 overall loss due to scams, adjusted to account for underreporting, was $158.3 billion.[10] Further, Bankrate recently found that more than one in three (34%) Americans experienced some type of financial fraud or scam in the past year (January 2024-January 2025). The survey also revealed that 68% of Americans have experienced a financial scam or fraud in their lifetime.[11]

Partnering with law enforcement at the local, state, and federal levels is also critical to countering the fraud and scam crisis our nation faces. Where crimes are reported, as Miami-Dade County Sheriff Rosie Cordero-Stutz can attest, they often present as single incidences below prosecutorial thresholds. Yet, with the ability to connect dots at the state and federal levels, the ties to larger, and even transnational, criminal organizations are clear.

The FBA is working with the Florida Attorney General's office to explore establishing a Financial Crimes Intelligence Center or dedicated financial crimes task force like the one employed in Texas. This effort would build on the great work already done in Florida with the cyber fraud enforcement unit. This entity could:

- Serve as a hub for investigations of financial crimes in Florida, connecting what would otherwise be handled as local, low-level crimes to larger scam rings and organized crime.
- Provide fraud-specific data analytics to detect cross-jurisdiction patterns.
- Work with local prosecutors to secure timely convictions.
- Streamline reporting processes across federal and state agencies.
- Support law enforcement with fraud-specific training and digital forensics capabilities.

Information sharing to further criminal investigations is a two-way street. Government has comprehensive reporting, whereas each financial institution only sees its piece of the puzzle. FinCEN and law enforcement need to feed banks and other stakeholders actionable, up-to-date information on the typologies, patterns, and characteristics of the illicit financial transactions that target consumers. Improving feedback loops to banks was one of the important reforms Congress included in the Anti-Money Laundering Act. We are gratified to see the initiative just announced by Internal Revenue Service - Criminal Investigation (IRS-CI) on March 28, 2025 to provide quantifiable results to financial institutions on IRS-CI's use of SARs, which will include a pilot site in Florida.

A Call to Action

I have focused on large-scale scams and fraud perpetrated by organized crime in my testimony. This Committee, however, knows well that older Americans often fall prey to manipulation from the very trusted individuals in their lives - friends, caretakers, family members. Bankers often contend with and identify these crimes as well.

Fraud is not just a banking problem - it is a societal threat that requires coordinated action. Florida's bankers are committed to protecting our customers and communities, but we cannot do it alone. As part of a comprehensive strategy, we need action from other sectors and from the government.

We are grateful for the leadership being shown by you, Chairman Scott, and the Aging Committee members in holding this hearing and continuing to shine a light on these horrific scams. Thank you once again for the opportunity to testify. I look forward to answering your questions.

[10] https://www.ftc.gov/system/files/ftc—gov/pdf/paddle-anf-statement.pdf
[11] https://www.bankrate.com/credit-cards/news/financial-fraud-survey/

U.S. SENATE SPECIAL COMMITTEE ON AGING

"PROTECTING FLORIDA'S SENIORS: FIGHTING FRAUD AND FINANCIAL EXPLOITATION"

AUGUST 7, 2025

PREPARED WITNESS STATEMENTS

Brandy Bauer

Thank you for inviting me here today on behalf of the Senior Medicare Patrol program. The nation's 54 Senior Medicare Patrol, or SMP, programs are managed by the U.S. Administration for Community Living, with the mission to help empower and assist people to prevent, detect, and report Medicare fraud, errors, and abuse.

Medicare fraud is a particularly insidious form of financial scam, because unlike other fraud schemes targeting an individual, the government and American taxpayers all pay the price. It's also challenging to detect Medicare fraud in real time, as there can be weeks or months between when Medicare is falsely billed for services and when an enrollee sees that charge show up on their Medicare Summary Notice or plan's Explanation of Benefits.

The Senior Medicare Patrol program model is one of prevention. SMPs educate millions of Medicare beneficiaries each year on how to guard their personal health information, scrutinize their medical statements and bills, and subsequently alert the program to any suspicious activity. The SMPs report cases of possible fraud, errors, and abuse to the Centers for Medicare & Medicaid Services and HHS Office of Inspector General, who then take up the investigation.

Here's just one real-life example of how this work plays out: Recently, a gentleman from Walton County, Florida was looking at his Medicare Summary Notice and discovered charges for urinary catheters and glucose monitoring supplies - equipment that he neither needs nor ever received. He reported this to the Florida Senior Medicare Patrol, who were able to help him get a new, uncompromised Medicare number. Yet Medicare had already paid over $15,000 for these fraudulent charges.

This beneficiary was observant; think how many times this scenario takes place across Florida and the country and goes undetected. As such, it's hard to get a concrete calculation of how much Medicare fraud costs Americans each year, but estimates put it in the tens of billions of dollars.

Because the Senior Medicare Patrol relies heavily on trusted volunteers from the community - in many cases, older adults themselves - the SMP program is often on the forefront of detecting emerging fraud trends. SMPs were among the first groups to spot unusual activity around fraudsters offering COVID-19 test kits in exchange for personal or medical information. Other emerging schemes the SMPs have helped identify include genetic testing scams, hospice fraud, and most recently, schemes related to remote patient monitoring and wound care. In addition to costing Medicare billions of dollars, some of these schemes can cause real patient harm, such as when a person falsely enrolled in hospice may be denied coverage for services that fall outside of palliative care.

The Senior Medicare Patrol is an Older Americans Act success story. First authorized under the OAA in 1997, the SMPs have provided outreach, counseling, and education about Medicare fraud to millions of older Americans. Since their creation, expected recoveries to Medicare (and Medicaid) attributable to the SMPs equals more than $287 million.

Medicare fraud doesn't exist in a vacuum. People vulnerable to other forms of financial exploitation may be at risk of unknowingly sharing their medical identity with health insurance fraudsters. Many of the same prevention strategies we hear from other sectors are relevant here as well - such an encouraging people with Medicare to guard their medical identity just as they would their Social Security or banking information, hang up on unsolicited calls, and report suspicious activity to the authorities.

The Senior Medicare Patrol's efforts not only serve to enhance the financial, physical, and mental well-being of older adults, but also to preserve the integrity of Medicare. I'd like to thank the Chairman and Senate Aging Committee for including our program in this important conversation today.

○