Written Testimony
U.S. Senate Special Committee on Aging
Hearing: "Fighting Fraud: How Scammers are Stealing from Older Adults"
Scott Pirrello
Deputy District Attorney, Head of Elder Abuse Prosecutions
San Diego District Attorney's Office
September 19, 2024

Good morning, Chairman Casey, Ranking Member Braun, and other members of the Senate Special Committee on Aging. I appreciate the opportunity to share my testimony with you today.

My name is Scott Pirrello. I am originally from Long Island, New York and I attended Penn State University. However, I am now a career Elder Abuse Prosecutor for the San Diego District Attorney's Office. In 2018, I felt a call to action after an epiphany that despite being the Elder Abuse Prosecutor for our county that I was seeing ZERO elder scam cases come across my desk even though I was contacted by dozens of victims whenever I was out in the community. When I sought out the answer to the question of why I had zero cases, I was shocked to learn that hundreds of reports existed, but once local police determined that the bad guys were far away overseas, the cases were filed away and never submitted to local prosecutors.

I assumed then, like so many, that certainly someone or some agency was in charge of working on these cases, someone was caring about all these untold victims, and someone was working to stop this problem from happening. I was wrong.

Right at this moment, there are thousands of American seniors all throughout the country being scammed – they are grandparents, aunts and uncles, friends and neighbors, veterans, best-selling authors, engineers, retired teachers and police officers. They are living independent and vibrant lives. They still live in their own homes, still drive a car, help out their families, and volunteer in their communities. And this morning as I testify, they are being terrorized by foreign nationals, on the verge of having their lives destroyed and forced into financial ruin.

This morning as each of them logged onto their computers to check in on their grandchildren or to glance at Facebook, a simple popup message appearing to be from Microsoft may have appeared on their computer screen saying that something was wrong with their computer and that they needed to call a given phone number to fix it. This phone number is often spoofed to appear like a number local to the victim. The scammers, often posing as helpful Microsoft support folks, then convince those seniors to accept a download of a remote access software onto their devices, which authorizes a trojan horse to allow the scammers to see inside their computer. Next the scammers begin to instill fear into their victims by telling the victims that their computers have been hacked and their information has been used for some horrific purpose, such as to view child sexual abuse material, or has been involved in some illegal drug cartel activities.

Once the scammers have access to their devices, the scam shifts towards their finances. The fake Microsoft worker tells the victim that their financial accounts have also been hacked and must be secured. The scammer then transfers the call to a "colleague" – another scammer posing as a

representative from a bank security department, the United States Department of the Treasury, Federal Trade Commission (FTC), U.S. Marshalls, or any other federal agency.

The fleecing has begun, and the next ask is a test of whether the scammer has the victim hooked or not. The victims are instructed to withdraw a high value of money, like $30,000 or more, from their bank – or they are told to purchase gold bars worth $20 to $40 to $60,000. Once the victim has the cash or the gold secured, they are instructed to either send cash through Bitcoin ATM machines or to package it up in cardboard boxes and instructed to either ship it across the country, or they are told that a courier posing as a federal agent will be coming to their house to pick up the package. This will continue until the victim runs out of funds, or until someone interferes.

The scenario I just described is not fictional. This narrative is exactly what occurred in our most recent case in San Diego last week. A 94-year-old Air Force Veteran lost $143,000 in five separate pickups of cash over a two-week period. According to the FBI's most recent Elder Fraud Report, tech support scams were the most prevalent scams perpetrated against older adults.

Hundreds of thousands of victims from all around the country fight through the humiliation and shame these scams cause each year, and summon the courage to report what has happened to them. They will call their banks and then reach out to their local police departments, their local prosecutors offices, to the Federal Bureau of Investigation (FBI), FTC, or to their State's Attorney General's and Consumer Protection Offices, or perhaps they will try to contact the U.S. Department of Justice (DOJ)'s Transnational Elder Fraud Strike Force, a program highly promoted by the Department of Justice as a potential solution to this scam activity. But these victims will all be met with the most regrettable answer: they will be told, "I'm sorry, but there is nothing that we can do."

I am here today speaking on behalf of the MILLIONS of American elder fraud victims in recent years who have been begging their government, local and federal law enforcement, and the banking, technology, and retail industries to help them. Too many very well intended programs are not implemented in a way to truly impact the tsunami of fraud that we are facing each day.

Currently, we are all failing the very people who need us the most: older adults – many of whom can't afford to lose anything, let alone everything. We are failing in our most basic duties to protect those in their golden years who are living off the nest eggs they worked for their entire lives and who are beyond the ability to rejoin the workforce to make the money back. These are lives in ruin.

Another failure of the status quo is the inability to accurately report on Elder Fraud victims and loss amounts. Without a mechanism for centralized reporting and accounting for all reported cases from all available sources along with reasonable estimates for unreported cases, policymakers are not making informed decisions on resource allocation. By all reasonable measures, the actual amount of losses each year attributed to elder scams in this country likely exceeds one hundred billion dollars.

Since 2019, on the backs of a few patriotic former Marines working in our DA's office and the San Diego's FBI office, we have been working to change this narrative and prove that contrary to the strategy of surrender, something COULD be done to fight this siege on older adults. To fight the status quo, we had to develop methods and strategies to at least mount a counterstrike.

In 2021, under the leadership of San Diego County's elected DA, Summer Stephan, our office worked with the San Diego FBI to launch a first of its kind Elder Justice Task Force to combat elder fraud. While it was previously thought that all fraudsters were overseas and out of the reach of law enforcement, we have since learned that scammers abroad depend on very organized networks of money launderers operating here within the United States. There are thousands of criminals within these networks who need to be investigated and prosecuted, yet there is no effort outside of ours in San Diego that is dedicated to focusing on these organizations.

The San Diego FBI Elder Justice Task Force (or, EJTF) brought together partners, including the San Diego County District Attorney's Office, the FBI, Adult Protective Services (APS), the DOJ, and our local U.S. Attorney's Office, all local law enforcement agencies, as well as the San Diego Law Enforcement Coordination Fusion Center ("LECC") to work together in an unprecedented fashion to connect the dots and turn small, local fraud investigations into large scale federal investigations and prosecutions. By eliminating the barrier of financial thresholds, the success of each of our EJTF investigations begins with a single local victim using a traditional investigation strategy. Cases are then built through collaboration and utilization of all local resources from APS and law enforcement, coupled with the FBI's incredible capabilities to extend the reach of our investigations outside of our county and throughout the United States, when necessary. Most of these assets of the EJTF are collocated working out of one physical location in San Diego.

The EJTF is now committed to serving these core functions: 1) investigating criminal organizations committing or facilitating fraud within the United States and holding those perpetrators accountable with both state and federal prosecutions; 2) regardless of whether a criminal investigation or prosecution is occurring, working to recover and return funds lost by elder victims wherever possible, including a new aggressive effort to use federal seizure warrants to recover millions of dollars lost by elder fraud victims; 3) collecting and reporting data on the amount of fraud impacting the County of San Diego broken down by jurisdiction; and 4) educating the community, both public and private sectors, about the current greatest threats.

The San Diego EJTF is the only initiative in the nation that is proactively responding to actual elder fraud cases in real time because we are tracking each report of fraud in our county collected by local law enforcement, FBI's IC3.gov database, and APS. We are talking every day to new victims and learning about the new scams and tactics the scammers are using to hook victims. This constant, real-time review of scam reports enables us to lead other agencies, localities, and states when it comes to identifying new scam trends and understanding how these transnational criminal organizations are functioning.

For instance, we have identified tech scams originating in Indian Call Centers as the greatest current threat to our seniors in San Diego and around the country. These scams are facilitated by money laundering cells, primarily made up of foreign actors, who are dispatched from a regional hub, as couriers, to pick up millions of dollars in scam payments.

In the past two years, the San Diego EJTF has worked to disrupt these networks. We have paired local investigators and APS workers with FBI agents to target these networks and we have had success: we have arrested over a dozen of these couriers. We are now routinely filing state prosecutions on these couriers, which have resulted in several federal indictments, including July's indictment by the US Attorney's Office in San Diego of a money laundering ring responsible for receiving stolen funds from over 2,000 victims totaling $27 million in elder fraud losses.

Despite these successes, the data is astonishing and shows how much work there is still to be done. In our county, we were shocked to see that the amount of losses doubled from 2022 to 2023, with $98 million from elder victims lost in 2023. Even more shocking is the reality that despite our progress, we are only able to work on one tenth of one percent of the cases we see.

Investing in education, as well as funding task forces like the EJTF, are critically important components in this fight against scammers. Both must be funded adequately. However, we cannot educate ourselves out of this problem nor can we prosecute our way out of this problem.

The only approach that could truly bend the curve resulting in more victims and losses each year will be a holistic whole of nation strategy, similar to what has been assembled in the United Kingdom and Australia in recent years, to identify every opportunity both upstream and downstream of the scam and work to stop the threats. This approach will ultimately eliminate the scammers' ability to attack our seniors on the technology we depend on, make the fleecing of financial accounts more difficult to accomplish, and provide support to the countless Americans who have reported their cases but have never heard back from a single person.

The cause of fighting Elder Fraud does not have a face. It is too siloed and unorganized. The U.S. Senate Special Committee on Aging should take this opportunity to lead and work with all relevant decisionmakers to urgently ensure that not one more victim falls prey to these scams. Through my work, I have seen that our goal should be loftier than creating programs, accumulating data, and writing reports. We can stop this problem entirely and I'm dedicated to joining the Committee in this fight. Every single one of us can do more for these victims, especially for the vibrant grandmother or grandfather who is going to wake up tomorrow to a popup ad from a scammer on their computer. What will be our answer when that victim calls us for help?

**For reference, I will direct you to a submission for the record prepared by another leading advocate in this cause, Ken Westbrook. Mr. Westbrook retired after 33 years in the CIA and is currently the Chief Executive Officer of the Stop Scams Alliance. The Stop Scams Alliance has highlighted the success of other countries, like the United Kingdom and Australia, at stopping scams at the source, and shown how the United States can model these successes.