Pennsylvania Attorney General Josh Shapiro

Testimony before the United States Senate Special Committee on Aging

October 4, 2017

Introduction

Chairman Collins, Ranking Member Casey, and members of the Committee, I am Josh Shapiro, Attorney General for the Commonwealth of Pennsylvania. Thank you for inviting me to speak with you today about what my office is doing to keep senior citizens safe from scam artists and financial predators and what steps the Federal government can take to further protect the elderly from financial exploitation.

The well-being of our nation's 47 million seniors is an important issue. As an elected official from Pennsylvania, it is particularly important to me. Pennsylvania has one of the highest populations of seniors over the age of 65 in the country: there are 2.2 million seniors in Pennsylvania—the fifth highest number in the U.S.—accounting for over 17 percent of our total population. And our population of seniors is only expected to grow, increasing by 25 percent by 2020.

As the chief law enforcement officer of the Commonwealth of Pennsylvania, I am responsible for protecting all Pennsylvanians in their roles as consumers. My responsibilities range from antitrust to home improvement contractors, from civil rights to managing our state's Do Not Call list. Protecting vulnerable seniors from unscrupulous scammers is one of my most important duties.

In my testimony today, I would like to cover three main topics: (1) seniors' vulnerability to scams and the impact scams have on them; (2) IRS impersonation scams; and (3) Pennsylvania's Do Not Call registry, which complements the federal system, and its effect on robocalls.

Seniors' vulnerability to scams

Senior citizens are specifically targeted for fraud and scams more than any other age group. Many of the most common scams are tailor-made for their specific life circumstances, including those involving Medicare, prescription drugs, funerals, anti-aging products, and grandparent scams. Understanding why seniors are vulnerable, and why they're being targeted, is necessary to developing solutions to better protect them.

Why seniors are more vulnerable

Seniors are now easier to reach than ever: according to a recent study from Pew Research Center, 67 percent of seniors have some form of internet access; 74 percent live in homes with computers; 51 percent access the internet through high-speed connections; and 34 percent of seniors who use the internet use social media (such as Facebook), making them even easier for scammers to locate and contact. Compounding this is seniors' comfort with conducting financial transactions online. Whereas 15 years ago, online financial transactions were relatively rare and viewed by the general public with skepticism, a recent study indicates that today 41 percent of seniors bank online, 26 percent pay their bills online, and 21 percent file their taxes online.

This is also the wealthiest generation of seniors perhaps ever. According to Nielsen, they have a median net worth of $241,333. That's 34 percent more than the

"War Babies" generation (born 1936 -1945) and 39 percent more than "Depression Babies" (born 1926-1935). In the words of the AARP, a scammer would "have to be an idiot to turn [their] back on this humongous market."

Impact

The combination of scammers' greed and seniors' vulnerability has resulted in significant financial losses for America's elderly. Over a third of seniors have experienced some form of financial abuse, including scams. Victims lose an average of $36,000. While it is difficult to calculate, our best estimates indicate that American seniors lose over $3 billion each year to scams and abuse. Two-thirds of seniors report having been victimized online: 38 percent have been targeted for online scams, and 28 percent have mistakenly downloaded a virus.

Discussing the impact of these scams in terms of billions of dollars or percentages of victims obscures the real impact on individuals. The loss of even a few thousand dollars can be devastating to a senior citizen. Nearly a million seniors in the United States have been forced to skip meals because they lost money to a scammer.

NAAG focus

Protecting seniors from scams and fraud is an important issue in every state, and attorneys general are making it a top priority. In August, the new president of the National Association of Attorneys General (NAAG), Kansas Attorney General Derek Schmidt, announced that NAAG will spend the next year focusing on "strengthening efforts nationwide to combat elder abuse." To quote Attorney General Schmidt, "There is no partisan divide on the commitment of state attorneys general to protecting seniors and combating elder abuse in all its forms."

OAG's efforts

The Pennsylvania Office of Attorney General (OAG) dedicates significant resources to consumer protection. Of our nearly 20,000 complaints from consumers each year, one third come from seniors in our Commonwealth. OAG receives and investigates complaints from seniors regarding:

- Purchase of goods and services (*e.g.* automobiles, pets, and insurance)
- Deceptive trade practices (*e.g.* false advertising or odometer tampering)
- Health care (*e.g.* health insurance service denials)
- Home improvement contractor scams
- Identity theft

In addition to this reactive work, OAG conducts proactive educational outreach to prevent seniors from becoming victimized in the first place. We have a dedicated Office of Public Engagement that manages this programming. Examples of some of our presentations most of interest to seniors are:

- Scams, fraud and identity theft education

- Senior Crime Prevention University, a specialized series of educational sessions for seniors to identify and avoid scams
- Cyber security for seniors

Finally, OAG manages Pennsylvania's Do Not Call list, which guards against unwanted marketing calls.

Throughout these various efforts, the most common complaints we receive from seniors are about violations of the Do Not Call list, including robocalls. The next most frequent complaints are about telecommunications and broadcast issues (including television and internet service providers), home improvement contractor issues, and scams like IRS impersonation.

IRS impersonation scams

IRS impersonation scammers call people and falsely claim to represent the Internal Revenue Service. The callers will claim that back taxes are owed by the recipient, threaten to have them arrested, and demand payment (usually via wire transfer). Last year, my office received 881 complaints about and IRS impersonation scams, 62 percent of which were from seniors.

Fortunately, most Pennsylvanians are able to recognize these calls as fraudulent. In the past, it helped to know that the IRS did not call people about their taxes, and that they only sent letters; however, as of April, Congress authorized the IRS to begin contracting out some of its debt collection work to private debt collectors who do make phone calls, which takes this defensive knowledge away. While there are some safety measures in place, like a passcode sent by mail that the caller must provide to a senior, I fear that ending the simple rule that the IRS will not call opens the door to more successful scams by sophisticated con artists.

John's story

In May of this year, agents in my office received a complaint from a man from the Pittsburgh area. I will call him "John" to protect his identity, as this investigation is ongoing. John received a call from a 1-866 number who claimed to be an IRS employee. The caller said that an arrest warrant had been issued for John because he sends money to his wife and child in a foreign country. The purported IRS employee said that John would soon receive a call from the local police department and instructed him on how to merge the calls. Shortly thereafter, John received a call from a number that his caller ID showed as coming from Pennsylvania State Police Headquarters.

The callers threatened John and said that his only way out of the situation was to send money to help pay for the investigation to clear his name. The money, they said, would be refunded to John after the investigation was complete.

John believed them, since they appeared to be calling from legitimate phone numbers. He was instructed to send six different payments from four different locations—Walmart, CVS, Western Union, and Rite Aid—over two days. In total, he lost

$13,500 because he truly believed he was speaking with tax authorities and wanted to clear his name. John's story demonstrates just how manipulative and devastating IRS impersonation scams can be.

OAG's efforts – grassroots education

Unfortunately, cases like John's can be difficult to prosecute. Anonymous criminals hiding behind spoofed phone numbers using shady financial transactions leave little for law enforcement to work with. That's why one of the best approaches to battling scams like this is preventative education.

My office takes a grassroots approach to educating seniors on how to identify and avoid scams like the IRS impersonation scam. Each year, we hold around 250 events all across Pennsylvania, reaching 14,000 seniors. Additionally, we hold 50 events on identify theft for people of all ages that reach approximately 5,000 additional seniors. These presentations teach seniors about a wide variety of scams and how to recognize and avoid them. We have also begun to incorporate materials on how to be safe while using the internet, as more and more seniors go online each year.

Many seniors are aware of the most well-known scams. As a result, these scams have very low success rates. This Committee estimated that last year one million Americans were targeted with the IRS impersonation scam, yet only 5,000 were victimized—a 0.5 percent success rate. However, many scams are not well-known, and new scams are popping up on a regular basis. So during our info sessions, we focus on communicating two crucial strategies for avoiding scams.

The first is an easy way to remember how to recognize a scam. Our agents have developed a pneumonic around the word "scam" itself: Sudden Contact, Act now, Money or information required. We tell seniors that if they are suddenly contacted by someone that they weren't expecting, and that person is demanding that they act immediately by sending money or information, then it is likely a scam.

The second is a simple, yet effective technique. If you don't recognize a phone number that's calling you, let it go to voicemail or your answering machine. Especially for seniors with diminished mental faculties, taking the time to listen to a message a couple of times, think about it, and even ask someone else for their advice can be the difference between avoiding a scam and losing thousands of dollars to a criminal.

Pennsylvania's Do Not Call list and robocalls

Under Pennsylvania's Telemarketer Registration Act, my office administers a free Do No Call list service for both landlines and mobile phones. Pennsylvanians can sign up by completing a simple form on our website. We collect those numbers into a list that businesses must reference before placing solicitation calls.

There are currently 3.5 million Pennsylvanians registered on the Do Not Call list out of a population of 12.5 million, nearly 30 percent. The list contains 2.8 million phone

numbers. The number of registered numbers is lower than registered individuals because multiple people from the same household can register the same phone number.

Despite the wide use of Pennsylvania's Do Not Call list, we receive thousands of complaints each year alleging unlawful telemarketing, robocalls, and scam calls. Last year, we received over 7,000 complaints, nearly 4,000 of which were from seniors. Many seniors that we talk to feel that the Do Not Call list is ineffective because they still receive unwanted marketing calls.

The Do Not Call list is not a panacea. While nearly every business complies with its restrictions, there continue to be a handful of bad actors who ignore it. There are also some major exceptions to the restrictions: political campaigns and nonprofits are not subject to the Do Not Call list, and any business that has had a business relationship with an individual in the last 12 months may disregard their placement on the Do Not Call list. Scammers also ignore the Do Not Call list; after all, it's often the least of the many crimes they're committing.

Still, the fact is that the Do Not Call list drastically reduces the number of unwanted calls that seniors receive and makes it easier for them to ignore calls from unknown numbers.

Again, our office recommends that seniors let any unknown number go to voicemail. This strategy lets them assess the validity of the call. Answering a call also lets the company calling know that the number is still active, and they'll keep it on their list to call again. Devices that screen calls automatically are also helpful in reducing seniors' vulnerability to scams.

OAG's efforts

In 2016, my office received 4,473 consumer complaints specifically relating to the Do Not Call list. Since then, my office has issued 2,141 subpoenas to phone carriers to try to locate calling parties. However, this resulted in only four legal actions, highlighting how difficult it is to pursue these cases. When we are able to build a complaint, though, we can build strong cases and obtain meaningful relief for those affected.

For example, last year my office took action against a man from Oregon named Richard Paul, alleging violations of Pennsylvania's Unfair Trade Practices and Consumer Protection Law and Pennsylvania's Telemarketer Registration Act. Our office alleged that Mr. Paul obtained telephone numbers for the purposes of conducting marketing calls. Many of the people he called were on Pennsylvania's Do Not Call list; our office received several complaints about his conduct as a result, including from seniors. This case is still pending; we are currently seeking remittances of $100 per affected consumer and civil penalties of $1,000 per violation or $3,000 per violation against a senior.

Steps the Federal Government can take to protect seniors

Prevent IRS private debt collectors from calling

As mentioned earlier, we used to be able to tell seniors that if someone was calling claiming to be from the IRS, then it was a scam—period—because the IRS does not call anyone. However, with the IRS's new private debt collection practices that began in April, it is possible for people to receive legitimate calls seeking to collect on debts to the IRS. This is causing confusion in our communities, and has removed a crucial method of self-defense.

Congress should look closely at the effects of permitting debt collectors working on behalf of the IRS to make telephone calls to people from whom they are collecting debt. The IRS has used other means for decades and never felt the need to turn to phone calls. I believe their debt collectors should adhere to the same practices.

Give telephone companies the tools to block scammers

According to the *Consumer Sentinel Network Data Book for January-December 2015*, 75 percent of consumers who filed fraud-related complaints and reported how the fraud was perpetrated indicated they were contacted by telephone. This is more than nine times the number reporting fraud initiated by e-mail (eight percent) and more than 12 times the number of those reporting fraud triggered by the internet (six percent). This statistic reveals that the telephone remains a potent instrument for criminals who are intent upon defrauding consumers.

I appreciate and applaud the efforts of the telecom industry to try to stop scammers in their tracks. I recognize the difficult balance that they must achieve between maintaining free and open lines of communication for all Americans and closing off avenues for harassment and scams. As is the nature of nearly every criminal activity, it is a constant battle to keep up with new methods and new technologies used by bad actors to circumvent the systems in place to protect us.

That's why the federal government needs to give telephone service providers the ability to block several kinds of "spoofed" calls (in which scammers mimic the phone numbers of legitimate businesses on the receiving party's caller ID). In July, I joined a bipartisan coalition of 29 attorneys general from across the country to submit a formal comment to the Federal Communications Commission asking them to allow telephone companies to block certain robocalls and spoofed calls.

As we said in our FCC comment, telephone companies should be able to block calls originating from "spoofed" or invalid numbers, unallocated numbers, and numbers whose owners have requested be blocked. For example, phone providers would be able to block a scammer that is using a telephone number that clearly can't exist because it hasn't been assigned. Legitimate businesses do not need to use any of these spoofing methods to contact consumers. Allowing providers to block these calls would stymie scammers without burdening businesses.

I know Senator Casey shares my views on this issue. He and I are sending a joint letter to the FCC today to implement their proposed rule without further delay. It has been nearly eight months since the FCC first proposed the rule. During that time, it is likely that 19 billion calls have been placed using robocalling technology. We need the FCC to help us put a stop to these harassing and predatory calls.

Conclusion

Thank you Chairman Collins, Ranking Member Casey and all the members of this committee for holding this hearing and highlighting the issue of scams and fraud against our seniors. This is a top priority for my office and I appreciate your focus on it here in Washington. I look forward to answering any questions you may have.