S. HRG. 116–544

COMBATTING ROBOCALL FRAUD: USING TELECOM ADVANCES AND LAW ENFORCEMENT TO STOP SCAMMERS AND PROTECT SENIORS

HEARING

BEFORE THE

SPECIAL COMMITTEE ON AGING

UNITED STATES SENATE

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

WASHINGTON, DC

JULY 17, 2019

Serial No. 116–10

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

47–365 PDF WASHINGTON : 2022

SPECIAL COMMITTEE ON AGING

SUSAN M. COLLINS, Maine, *Chairman*

TIM SCOTT, South Carolina	ROBERT P. CASEY, JR., Pennsylvania
RICHARD BURR, North Carolina	KIRSTEN E. GILLIBRAND, New York
MARTHA MCSALLY, Arizona	RICHARD BLUMENTHAL, Connecticut
MARCO RUBIO, Florida	ELIZABETH WARREN, Massachusetts
JOSH HAWLEY, Missouri	DOUG JONES, Alabama
MIKE BRAUN, Indiana	KYRSTEN SINEMA, Arizona
RICK SCOTT, Florida	JACKY ROSEN, Nevada

SARAH KHASAWINAH, *Majority Acting Staff Director*
KATHRYN MEVIS, *Minority Staff Director*

C O N T E N T S

COMBATTING ROBOCALL FRAUD: USING TELECOM ADVANCES AND LAW ENFORCEMENT TO STOP SCAMMERS AND PROTECT SENIORS

WEDNESDAY, JULY 17, 2019

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

The Committee met, pursuant to notice, at 9:32 a.m., in Room 562, Dirksen Senate Office Building, Hon. Susan M. Collins, Chairman of the Committee, presiding.

Present: Senators Collins, McSally, Rubio, Hawley, Braun, Rick Scott, Casey, Blumenthal, Jones, Sinema, and Rosen.

OPENING STATEMENT OF SENATOR SUSAN M. COLLINS, CHAIRMAN

The CHAIRMAN. The hearing will come to order.

Good morning. Protecting American seniors from scammers who seek to defraud them is a central goal of this Committee. In the past 6 years, we have held 23 hearings on frauds and scams targeting our seniors. Using just phones and the Internet, fraudsters have proven to be relentless. To protect our Nation's seniors, we must continue not only to prosecute con artists who steal literally billions from our seniors, but also to find new, more effective ways to block illegal spoofing and robocalls at the network level.

Last year, robocallers generated more than 26 billion unwanted calls that reached Americans' mobile phones. When landlines are included, the number soars to 48 billion. In Maine alone, our residents received an astonishing 93 million robocalls last year. That is an average of 73 calls to each person in our State, so far this year, scammers are on pace to generate more than 58 billion unwanted, illegal robocalls targeting American consumers.

These scams overwhelmingly are initiated by offshore robocallers who are using new technologies to perpetuate their schemes. Today we will focus on a practice called "spoofing." This allows scammers to mask their identity by replacing the Caller ID tied to their actual phone number with one that fits their story. When victims see the "Internal Revenue Service" or the "local Sheriff's Department" pop-up on their Caller ID, they understandably answer the phone. They also are worried, scared, and often easily hustled into doing whatever the scammers demand.

With the emergence of the modern Voice Over Internet Protocol technology—or "VoIP," criminals can now operate from call centers

anywhere in the world—as far away from American law enforcement as they can possibly get—using VoIP to hide their identity while generating millions of robocalls at a very low cost.

Our Committee has called on regulators and the business community to work together more aggressively to stop scammers from using VoIP and other technologies to facilitate fraud. We have seen some progress on that front. US Telecom developed Traceback, a program to identify the source of illegal robocalls. Carriers are working to implement new technology called "SHAKEN/STIR" that will allow consumers to tell whether or not the Caller ID that shows up on their phones is legitimate or has been spoofed. But the implementation and the cost of these technologies to protect consumers has been slow.

On the positive side, we are seeing a more aggressive and coordinated approach against robocallers by the Federal Government. In 2016, the Department of Justice led a Federal investigation that closed down five call centers in India. A few weeks ago, the Federal Trade Commission and its law enforcement partners announced Operation Call it Quits, a major crackdown against foreign and domestic defendants allegedly responsible for more than a billion calls to consumers nationwide.

The Federal Communications Commission has also been more active.

These Federal actions represent progress that our Committee has pressed for to crack down on robocallers. Now the Committee is calling for a next generation approach—not only to crack down on the criminals, but also to consider new network-wide solutions to prevent robocall spoofing frauds in the first place.

We have recently taken an important step in the Senate by passing the TRACED Act, of which I was proud to be a cosponsor. I hope it will be signed into law soon.

Today, along with many of my colleagues, I am introducing the Anti-Spoofing Penalties Modernization Act, which will complement the TRACED Act's provisions on robocallers by doubling existing penalties and by extending the statute of limitations on prosecuting illegal spoofing.

Despite all of these efforts, the number of robocalls is expected to soar. To defeat these scammers, we need new technological approaches. We know from experience that the scammers are ruthless and relentless, and as long as these fraudsters can access our telephone network, they will continue to flood our phones with billions of calls in search of new victims. The key to defeating these scammers is to block the illegal robocalls from foreign call centers closer to their source before they can reach the American consumer. Today we will learn about new network level approaches with the potential to ultimately stop robocall spoofing fraud altogether.

Beyond the technology—and we will be reminded of this today—we must never forget that our purpose is to protect the victims of these notorious scammers. Too many seniors continue to lose their hard-earned money and often their entire retirement savings to con artists.

Even worse, as we will hear today, these scams can shatter the lives of seniors and their families and impose a cost that cannot be measured in money alone.

I am now pleased to turn to our Ranking Member, Senator Casey, for his opening statement.

OPENING STATEMENT OF SENATOR ROBERT P. CASEY, JR., RANKING MEMBER

Senator CASEY. Thank you, Chairman Collins, for holding this hearing and also for your opening statement.

I know that many in our country are divided on a range of issues, but we are united as Americans in despising these robocalls.

For some, these calls have become more than just a nuisance. The con artists on the other end of the line often turn a conversation into a heist—literally.

They threaten our aging loved ones, and they rip away their hard-earned savings, and as we will hear today, these criminals can cause terrible tragedy. The perpetrators of these crimes must be pursued and prosecuted to the full extent of the law, and they should be behind bars.

I was pleased to support resources for the Department of Justice and the Federal Trade Commission to successfully engage in two of the largest coordinated sweeps of companies facilitating these calls and the criminals making them.

Unfortunately, even these actions that took place earlier this year have not deterred the con artists. As one of our witnesses, Sheriff Sanders from Pennsylvania, will explain, some fraudsters only seem ever more emboldened.

They rig phone lines so the number that shows up on Caller ID appears to be the number of a local police or sheriff's office. Sheriff Sanders and local law enforcement officials across the country do not take such impersonation lightly.

These schemes are requiring an investment of time and resources from officers across the country. Instead of focusing only on what they do best—keeping our streets and our communities safe—local law enforcement officials must spend precious time keeping the phone lines safe.

This is one of the reasons why I am pleased to have introduced, with Senator Moran, the Stop Senior Scams Act just recently. This bill would create another line of defense against scammers by giving bank tellers, cashiers, and others the tools to spot a scam and prevent—prevent—someone from ever handing over cash to a stranger on the phone.

We hope that this bill is enacted swiftly. Much of what we will discuss today is how these crimes occur, but we must not forget the important role that both industry and regulators play in preventing an illegal robocall from being connected in the first place, and so we must make sure that the rules are in place to allow industry to adopt and to implement the most up-to-date call authentication and blocking technologies.

I am pleased that the Senate recently passed the TRACED Act, as Senator Collins referred to, and that the Federal Communications Commission recently finalized new rules to help get this technology to every consumer with a telephone, but as we will hear

today, we have a lot more to do. The mental and financial health, indeed the very well-being, of our loved ones is at stake.

I look forward to hearing more from our witnesses. We thank our witnesses. And I also look forward to working with Chairman Collins and other colleagues to put an end to these destructive calls.

Thank you, Madam Chair.

The CHAIRMAN. Thank you very much, Senator Casey.

I also want to thank Senator Scott of Florida for being with us today. He has been a very active member of the Aging Committee, and we are very happy to have him here.

We will now turn to our witnesses. Our first witness is Angela Stancik, who joins us from Texas. She is the granddaughter of Marjorie Jones of Lake Charles, Louisiana. Today Ms. Stancik testifies in memory of her grandmother and as a voice for the scores, the hundreds of Americans who have fallen victim to elder fraud.

I will now turn to the Ranking Member to introduce our witness from the Commonwealth.

Senator CASEY. I am pleased to introduce Sheriff Jerry Sanders from Drexel Hill, Pennsylvania. Sheriff Sanders has served as sheriff of Delaware County since January 2018. He previously served as a sheriff's deputy in the city of Philadelphia and later retired as chief inspector. In addition to his law enforcement background, Sheriff Sanders is a minister in his church and is the chaplain at a local retirement community. As we will hear from his testimony, even law enforcement and religious leaders are not spared from getting tangled up in these robocalls.

I would also like to welcome the sheriff's wife, Juanita, who I think is right behind him, over his right shoulder, and his chief deputy, Mike Donohue, both of whom have made the trip to be with us today from Delaware County, Pennsylvania, right next to Philadelphia.

Thank you both for being here, and, Sheriff Sanders, I look forward to hearing your testimony. Thank you.

The CHAIRMAN. Thank you.

Our third witness will be Delany De Leon-Colon, a Postal Inspector who oversees the Criminal Investigative Unit of the United States Postal Service. Throughout her 15 years of service for the Postal Service, she has managed teams focusing on various forms of theft, fraud, and money laundering that frequently result from these robocalls.

Finally, we will be pleased to welcome David Frankel. Mr. Frankel is a telecommunications expert who has worked in high-performance computer and networking technology since 1974. He helped to implement the telecom industry's Traceback effort, which assists law enforcement in tracking down the origin of illegal robocalls.

Thank you all for joining us, and we will begin with Ms. Stancik.

STATEMENT OF ANGELA STANCIK, GRANDDAUGHTER OF SCAM VICTIM, GANADO, TEXAS

Ms. STANCIK. Good morning. Thank you, Chairman Collins, Ranking Member Casey, and other members of the Committee for inviting me to be here today. I am very honored. My grandmother, Marjorie Jones, was a victim of elder fraud. There are no words to express what she meant to me and my family and how much we

all loved and adored her. The examples of her faith and love cannot be confined to words, and she will forever be missed.

My grandmother was targeted and pursued nonstop by a ring of fraudsters. Over time, these individuals used creative and cunning tactics to gain her trust. They told her she had won a large cash prize and all she needed to do was pay the taxes and fees.

I first realized my grandmother was a victim of elder fraud by the last conversation I ever had with her. Reliving that phone call is very painful. She explained that she needed $6,000 wired to her as soon as possible. Her forceful tone and desperation was very upsetting. I could hear the panic in her voice, and she was very, very afraid.

This phone call set off many red flags, and everyone grew extremely concerned about her financial situation. We do not know of a single time in her entire life where she ever borrowed money from an individual. My father informed me that he had wired her $8,000 the week prior, and he assured me he was trying to find out what was happening. He mentioned his fears that someone was scamming her, but because she was so desperate and scared, he sent her the $6,000 she wanted anyway. Sadly, she died less than a week later.

It pains me to talk about my grandmother's horrific death because she chose to take her own life. It is extremely hard to imagine a loved one committing suicide, but she did, because these individuals preyed on her and on her good heart. Her golden years and the last chapter of her life was taken from her. It is clear to us that the circumstances that led to her death were caused by these criminals.

After her death we found out just how much these criminals had taken from her. We found hidden in a closet several bags full of wire receipts where she had been sending large sums of money overseas. My family visited these wire marketing services to talk with the clerks and discovered that they had warned her that this was not legitimate and they believed it was a scam. She continued to wire money, but used a different location.

We also discovered not only did they drain her of all the money it took her a lifetime to save, but that she had taken out a reverse mortgage on her home and she cashed out all of her life insurance. My grandmother died with $69 in her bank account.

In the summer of 2016, we were notified by the Department of Justice that the individuals who committed this crime against her were caught. One of them had been extradited from Costa Rica and was already in the sentencing phase for her punishment. I traveled from Houston to Charlotte, North Carolina, to read my victim impact statement to the court and to finally face one of the individuals who did this, because of that statement, I was invited to speak with former Attorney General Jeff Sessions in February 2018, when he announced the Elder Fraud Sweep. Since then, I have been contacted by many Americans who are facing this exact type of scam, and personally I know two other close family friends that have been impacted by the "grandparent scam" and the "medical debt collection scam."

On behalf of my grandmother, Marjorie Jones, I want to thank the Committee for hearing and exploring the growing and difficult

problem of fraud against the elderly. We live in a fast-paced, youth-oriented society, and elder issues are not high on the social agenda. But you have the ability to show great leadership by shining a light on this topic, so again, I thank you for your passion that has helped raise awareness. Thank you for recognizing that as a Government, as a society. and as individuals, we must increase our efforts to ensure that our seniors are protected from the criminals that prey on them. Our seniors in this country deserve to live out their lives with dignity and honor.

Thank you.

The CHAIRMAN. Thank you very much for your moving testimony and for your willingness to come forward and share such a painful, horrible story with us, because you have been willing to do that, I am sure that you have alerted so many around this Nation, and that is a tremendous way to honor the memory of your grandmother, so I thank you for your courage and speaking out publicly, and I am so sorry for what you and your family have endured. Thank you for being here.

Sheriff Sanders.

STATEMENT OF JERRY L. SANDERS JR., SHERIFF, DELAWARE COUNTY, DREXEL HILL, PENNSYLVANIA

Mr. SANDERS. Chairman Collins, Ranking Member Casey, and members of the Committee, I am Sheriff Jerry L. Sanders Jr., and I serve as the sheriff of Delaware County, Pennsylvania. Thank you for the opportunity to testify before the Committee about my office's experience with scammers using robocall and spoofing technologies.

The Delaware County Sheriff's Office experiences occasional reports from citizens about receiving scam or "robo" calls from unknown persons.

These scams vary, but the most common form is the caller claims the potential victim has missed jury duty, and there is a warrant for their arrest. The caller will identify themselves as a member of the sheriff's office, typically using a fake name. In one recent incident, the caller used the name of an actual deputy, going so far as to use the deputy's voicemail greeting as their own. If the sheriff's office is able to get a number from a potential victim, calling it back typically results in no answer. On occasion, someone will answer, but once they realize the call is from the sheriff's office and we are asking legitimate questions, they typically terminate the call.

Another aspect of this is the callers often use "spoofing" technology. This is when they are able to program the actual sheriff's office main number to show on the potential victim's Caller ID. This is often how we find out about the calls. The potential victim, in most cases people who realized something was amiss, terminates the call and calls back using the displayed number, which is the actual office number. We will tell them that this is a scam. The sheriff's office does not call people that we have business with, that it is either done through U.S. mail or in most cases in-person service by the deputy. In addition, under no circumstances would we ever ask for information over the phone and never ask for money or any other valuable thing to avoid obligation or arrest.

In two separate incidents that occurred over the last several months, professionals were targeted. The scammers convinced two of them that they were subject to arrest for missing jury duty. In one case, they were able to get the victim to travel to a bank to withdraw $3,000 and then on to retail establishments where she was instructed to purchase thousands of dollars in money cards or gift cards and ended up mailing them off. The victim's husband grew suspicions and looked on the sheriff's web page on the county website and saw the scam alert, but it was too late.

In the most recent case, a similar ruse was used, and they advised one of the victims, a 65-year-old doctor, that he was subject to arrest for not responding to a grand jury subpoena. They had him convinced enough that they had him on the phone for approximately an hour and had coaxed him all the way to a bank in Media, Pennsylvania, and that was approximately 10 miles and 20 minutes away, and they instructed him to withdraw $6,000. They advised him that he should stay on the phone, not answer or communicate with anyone, and to follow their instructions. His wife in the meantime grew suspicious and tried to call him repeatedly. When she could not reach him, she called the sheriff's office. With that call and information she was able to provide, we were able to contact the bank and actually intercept the victim as he was parking his vehicle and thwart the execution of the scam and saved the victim thousands of dollars.

In the most recent case, the victim was approached by the chief deputy, who was in plainclothes and arrived in an unmarked car. When the chief first approached, the man was skeptical as to who he was, saying that he had the sheriff's office on the phone. The scammer terminated the call by the time the chief took the victim's phone. Once the victim realized what had just happened, he explained that he was chiefly concerned about his medical license and that if he were to be arrested, that his license would be jeopardized, as well as his position as a medical director—losing sight of the fact that this was an elaborate ruse. With them keeping him on the phone, running him across the county, telling him to not speak to anyone, et cetera, this was, in fact, just a ruse. He was actually intercepted a block from the courthouse, with the building in view, but instead of going in to verify, he was actually going to the bank to withdraw the money. He then likely would have been directed to go the to a "federally authorized retailer" to purchase money or gift cards, which he would then be instructed to give all pertinent information over the phone, and in some cases to mail them.

In the three most recent cases, it is believed the scammers were able to gather personal information on the potential victims, two medical professionals and an architect beforehand, most likely from the web. This enhances the scammers' ability to convince the victim that since they know much about them that the call is legitimate. This gets the victim off balance, and with the threat of potential arrest and then the offer of the out by paying a fine, they opt for that to avoid "arrest."

Frequent targets are older persons who typically have great respect for authority and tend to be much more trusting.

These type scams circulate through the State. We will often see emails from other sheriffs' offices. In response, when we experience them, we push out press and social media notifications to warn the public, and we have a permanent alert on the county website.

Unfortunately, given the limits of manpower and resources, local law enforcement can do little to investigate these crimes to arrest. Often trying to keep the public aware to avoid victimization is the best we can do.

I was pleased to learn that Senator Casey has introduced legislation that would help train bank tellers, cashiers, and others about how to spot a potential scam victim and to intervene to stop it. In this way, they would serve as another line of defense, protecting our family, friends, and neighbors from these criminals. I also think that more must be done by the telecommunications industry to stop these callers from getting through in the first place.

Thank you for the opportunity to speak before the Committee today. I look forward to answering any questions you may have.

The CHAIRMAN. Thank you very much, Sheriff, for being with us today.

Ms. De Leon-Colon? Did I get it close? Colon, right?

Ms. DE LEON-COLON. Yes, correct.

STATEMENT OF DELANY DE LEON-COLON, POSTAL INSPECTOR IN CHARGE, CRIMINAL INVESTIGATIONS GROUP, U.S. POSTAL INSPECTION SERVICE, WASHINGTON, D.C.

Ms. DE LEON-COLON. Good morning, Chairman Collins, Ranking Member Casey, and members of the Committee. I appreciate the opportunity to testify on efforts to combat fraud.

My name is Delany De Leon-Colon. I am the Inspector in Charge of the Postal Inspection Service's Criminal Investigation Group. I oversee several national programs, including mail fraud.

Prior to arriving to Washington, DC, I was the Assistant Inspector in Charge of our Miami field office. In that role I, with authorities in Jamaica to investigate lottery and sweepstakes fraud. I began my law enforcement career with the Immigration and Naturalization Service, later with the Secret Service, before being appointed as a Postal Inspector in 2004.

Every day, consumers of all ages are bombarded by marketing pitches, promotions, and offers. As a law enforcement officer, I have seen how persuasive language and high-tech deception are used to catch the attention of consumers and convince them to part with their money.

Imagine your phone rings and the voice on the other ends tells you it is your lucky day. However, you must first pay a little cash, called an "insurance fee."

Once an individual has been persuaded to pay an initial fee, the scheme's operator takes the relationship to the next level, asking for yet more money, while emotionally isolating the individual from friends and family. Most of the victims we interview were not aware that call-spoofing technology existed. By their own admission, they overcame their doubts and bought into the caller's fabulous claims because of the information displayed on their Caller ID. Spoofed phone numbers were instrumental in leading victims to believe the call they received was for real.

The case in which Ms. Stancik testified was investigated by Postal Inspectors in North Carolina with assistance from the Federal Bureau of Investigation, Internal Revenue Service, Homeland Security Investigations, and prosecuted by the Department of Justice Fraud Section.

The investigation entailed an offshore call center run by Andrew Smith, a Jamaican national, and Christopher Griffin, a U.S. citizen, both living in Costa Rica. Smith and Griffin, along with others they supervised, posed as representatives of the Securities and Exchange Commission and Federal Trade Commission. They contacted consumers in the United States, claiming they had won a prize.

The Costa Rican call center took steps to conceal its true identity, using call-spoofing technology that made it appear the calls they made came from Washington, DC, which lent considerable weight to the scam. Other Internet-enabled technologies also played a part. At trial, one victim testified she was warned to keep paying as the caller knew where she and her family lived. He used images and other information from the Internet to make his point.

Payments to Costa Rica were sent by wire transfer or through money orders sent by mail or private couriers. Smith and Griffin also hired runners to meet victims at their homes to collect their cash.

Nine defendants were charged. Eight worked in the call center, while one was caught laundering funds between the United States and Costa Rica. Postal Inspectors identified approximately 1,800 people living who collectively lost more than $10 million just in connection with this particular case. One such person was Ms. Stancik's grandmother, Ms. Marjorie Jones.

Several defendants were extradited to the United States, while others were arrested within the United States. Three remain fugitives. Smith and Griffin were both convicted and, in April of this year, sentenced to more than 20 years in Federal prison. Ms. Stancik testified on behalf of her grandmother at the sentencing of one of the defendants.

The Inspection Service is aggressively investigating frauds where there is a connection to the U.S. Mail, even when the mail is not the first point of contact. We participate in the newly formed Department of Justice Elder Fraud Strike Force and have Inspectors working full-time in Jamaica and in EUROPOL in The Hague.

We also know an issue as broad as this requires efforts on many fronts. We engage with consumers of all stages of life to teach them how to recognize schemes and take steps to safeguard their finances, including how to contact service providers for help blocking these unwanted and unsolicited calls.

Again, I want to thank the Committee for holding this hearing. I applaud the Committee's efforts to address the issue of phone technologies that facilitate schemes and that give scammers an unfair advantage.

Thank you.

The CHAIRMAN. Thank you so much for your testimony and for the great work that you are doing.

Mr. Frankel, thank you for being here.

STATEMENT OF DAVID FRANKEL, CHIEF EXECUTIVE OFFICER, ZIPDX LLC, MONTE SERANO, CALIFORNIA

Mr. FRANKEL. Thank you and good morning, Senator Collins, Ranking Member Casey, and members of the Special Committee. My name is David Frankel; I am the CEO of ZipDX LLC, a provider of specialized telecommunications applications. I am honored to be here.

I note that this week we are celebrating 50 years since some smart Americans came together and put our own on the Moon. I would like to believe that two generations later we can collectively across industry and enforcement and regulation get our phone network back from the scammers that have taken it hostage.

In my remarks today, I want to share my perspective on illegal robocalls, including how they work technically and commercially and why they persist. I will attempt to convince you that this problem can be addressed through a cooperative and focused effort to stop robocalls closer to their source.

I have prepared a diagram that illustrates the path taken by most robocalls. Before I start, I want to make a critical point clear: There is no way to send a call, robo or otherwise, to a U.S.-based consumer telephone except by arrangement with a so-called originating provider here in the United States. In other words, robocallers located outside the United States, or inside, for that matter, must buy what is called "call termination" service from an originating provider to get their robocalls onto our U.S. network. Calls typically pass through multiple subsequent providers before reaching the telecom carriers that directly serve consumers.

These originating providers do not have to invest in any equipment. Standard computing resources can be used to process these calls, and those resources can easily be rented in the cloud. They do this with Voice over Internet Protocol and so are referred to as "VoIP providers."

The robocallers' approach is to place an enormous number of calls through his VoIP providers in the hope of finding a handful of victims. If a robocaller snags just $100 from each of 50 victims a day, he could collect $100,000 a month. He will need to hire a few humans to close each deal, but the magic of robocalling is that most of the work, making millions of very cheap calls in search of potential victims, is done by computer. Even after paying his staff and those phone providers, our example robocaller could be clearing 70 grand in profit each month. It is no wonder that this is such a profitable endeavor.

The select subset of VoIP providers that enable the robocallers are generally small operations with low overhead. On a monthly basis, a VoIP provider in this country serving multiple robocallers and placing 100 million robocalls onto the U.S. network could earn $50,000 to $100,000 in profit. Thirty such operators would account for 3 billion illegal robocalls each month.

The best place to stop this illegal traffic is with those providers where the traffic is most concentrated. As the illegal calls move through the network, they disperse and are commingled with other calls, making detection more difficult.

We should know the source of each call from its Caller ID, but that takes us immediately to the problem of spoofing. Illegal

robocallers and scammers go out of their way to choose a VoIP provider that allows them to play fast and loose with Caller ID. Ultimately, the new SHAKEN/STIR protocol that carriers are implementing will help make clear whether a Caller ID is authentic. But while we wait for that protocol, the telecom industry today has a process called "Traceback" to identify the source of a given call. Providers have records of each call handled by their networks. Working cooperatively, each provider, starting with the carrier that serves the called consumer at the bottom of my diagram, searches its records and identifies the next provider in the chain upward that passed the call to it until the provider who allowed the robocalls onto the network in the first place is reached.

Traceback used to be entirely manual and required subpoenas to each provider, taking weeks to months. Now the process has been automated and can be completed in days or even hours. We do not have to trace back billions or millions of calls. One successful example can get us to the source. By tracing back selected call examples from illegal robocall campaigns, the providers that allowed those calls onto the U.S. network can be identified and notified to take steps to stop the calls. Regulators must step in where providers refuse to mitigate the calls.

In closing, we must be prudent about who gets what kind of access to the U.S. telephone network. It makes no sense for a robocaller in India, identified only by a gmail address, to be placing huge numbers of calls that look like they are originating from all over the USA. VoIP providers within our own borders that allow that to happen are the best choke point to stop the illegal robocall scourge. We must engage those providers to be part of the solution rather than contributing to the problem.

I welcome your questions.

The CHAIRMAN. Thank you very much, Mr. Frankel. I am going to start with you because I feel strongly that, given the enormous creativity of these ruthless criminals, we need a technological solution that is closer to the source.

I have been trying to sort out—and that is why your testimony is so helpful—whose responsibility is it to try to identify these bogus, illegal robocalls, and you talked about that they are small operators, but that they choose a VoIP provider that allows them in, so whose responsibility is it? Is someone making a lot of money from allowing these calls into the system? We know the scammers are making billions of dollars, as your example shows. But talk a little bit about whom we should hold accountable.

Mr. FRANKEL. Certainly. Thanks for the question, so it is indeed these small VoIP providers that are allowing those scammers to make their calls. In the universe of telecommunications providers—and there are many, many hundreds, a few thousand of them perhaps, in this country—most of them are upright businesses, and they are providing various kinds of services to consumers, to other businesses that all have legitimate needs to use the telephone network.

There are a small number of VoIP providers that cater to the kind of traffic that is associated with robocalling, and there are illegal robocalls, and there are legal robocalls, so we talk about prescription reminders and school closings and things like that which

involve blasting out a lot of calls periodically, and those are legitimate robocallers, and there are providers that serve them.

Those same providers or providers holding themselves out to serve that kind of need are the ones that are also potentially conduit for these illegal calls, and those are the ones where we need to have our focus and they need to be called upon to be more diligent about to whom they grant access that allows the massive calling and the spoofing that we see in the illegal robocall domain.

The CHAIRMAN. Thank you. That is very helpful.

Let me just ask one other question. Is there a technological barrier that makes it difficult to identify these bad actors?

Mr. FRANKEL. Another great question, some might tell you that it is challenging to know what is a good call and what is a bad call. That is especially true because telecommunications providers generally do not have access to the content of the telephone call. That is private, and technologically they are not monitoring what is being said when a call is placed, so they do not know whether somebody is saying, "Your prescription is ready," or, "You have just won a giant sweepstakes." There are other characteristics that the telecommunications providers do have access to that can make it much more apparent and at least raise suspicions.

For example, when a customer is overseas, or even when they are in this country, and they are making massive numbers of calls and each one is from a different number, the Caller ID shows a different number, that is suspicious. Why would that be the case? Who would legitimately be doing that? If I am a school, I am going to use the same number for every call I place. If I am the pharmacy, I will have perhaps a group of my pharmacy numbers in my library, but I will not be using other random numbers, thousands, millions of them from all over the country, so there are those clues, and the provider has the technology to screen what number their customers are providing as the Caller ID when the call is placed.

There absolutely are technology approaches and solutions that can be applied if you choose to apply them. And you will know that, as I said, there are thousands of VoIP providers or providers of telecommunications services. These robocalls do not originate from the vast majority of them. They originate through a very small set of them, so we have an existence proof that they can be prevented.

The CHAIRMAN. Thank you very much.

Senator CASEY. Thanks very much.

Sheriff Sanders, I will start with you. You recently put an ad in the local people in Delaware County that we wanted to thank you for because you were providing a kind of public education campaign about this issue, and I have no doubt that that warning that you put in the paper prevented others from falling victim to this crime.

I guess the question I have for you is: What did you learn from that experience, Number one. Number two, how would you recommend other law enforcement, especially local law enforcement officials, engage in order to prevent this kind of crime from being perpetrated?

Mr. SANDERS. I believe that some agencies——

The CHAIRMAN. Could I ask you to turn on your mic, please?

Mr. SANDERS. When other agencies become aware of phone scams, I think that they should also make it known to the public.

I think that we should participate more in community service in terms of going into senior homes, senior residences, and speaking about phone scams and making people aware. I think it is a joint effort that we all should, as we say here, make a concerted effort to inform the most vulnerable portion of our population.

I believe that the danger in not doing so makes the job of law enforcement officers more dangerous because if people are paranoid about authority and legitimate authority and cannot tell the difference, our deputies, our officers on the street can be exposed to additional danger when they knock on the door and the citizen is paranoid about exposure to legitimate authority and overquestioning on both sides. The deputy may be there for a legitimate reason, may have a warrant, and deem the activity on the other side of the door as being suspicious enough to break, and here it is just a senior that has become so questioning because they have been exposed to a phone scam.

I think that this is contagious, and it can spill into other areas of law enforcement and make it more dangerous for our officers and also more dangerous for the public.

Senator CASEY. One thing you mentioned as we were talking earlier today in the back is the potential to create both danger but also doubt. In other words, when law enforcement approaches a citizen, they may have doubts about that law enforcement official or about the institution they represent because of the proliferation of this fraud.

Mr. SANDERS. Yes.

Senator CASEY. And you have run into that directly, I guess, in some way or another.

Mr. SANDERS. Well, before becoming sheriff, which is more administrative than hands on, I was a deputy for 23 years, and when you knock on a door and you show your identification when someone answers, if they are suspicious of that, that is a situation that could escalate, and it could stem from paranoia that began with phone scams.

Senator CASEY. Well, we appreciate the fact that you have brought real-life experience to this, not just from a distance but from what you and your deputies have had to encounter.

Your testimony also highlighted a situation where your deputies went to a bank to stop that resident from actually completing the transaction, which would have cost them thousands of dollars, and we are grateful for that. I have introduced a bill, as I mentioned, to help educate basically three groups of folks: bank tellers and others at financial institutions, individuals who work at wire transfer companies, and the third is those who work in a retail establishment.

Tell us about how that might have an impact and anything else you hope that we would do by way of policy change or legislation.

Mr. SANDERS. Well, I consider all of these things that we are talking about connected. Being here today, I think it is part of a multi-pronged, proactive effort to educate our seniors. I think that what we are talking about now should be part of our conversation wherever we are at, in the houses of worship, community centers, every level of government when they have the forum where the public can speak, they can inform the public, Federal as we are

doing now, State, local—from all corners, multi-pronged and concerted to alert our seniors. They need us to do that.

We also know that suspicion can be triggered by a senior that may have early onset dementia or some ailment that is associated with or more prevalent among our seniors, so we have to be there for them.

Senator CASEY. Thanks, Sheriff.

The CHAIRMAN. Thank you.

Senator BRAUN. Thank you, Madam Chair.

Normally, when we are talking about something like this, we do not have something as simple as a choke point. When you mentioned that, that really kind of converges on, you know, what the solution is to the problem. I have got several questions here, and this is directed at Mr. Frankel, if you could give me some quick answers. How long have scams been around before technology made it really easy. Has this been around since landlines, or is it——

Mr. FRANKEL. Thank you, Senator. To my knowledge, my own personal experience, going back decades, the phone network has been a conduit for scams of various kinds. In the beginning they were scams against the phone company. There was a technology called "blue-boxing" that scammers used to extract money from phone companies, to get around pay phone charges and things like that, so it is as old as that.

Senator BRAUN. The recent focus on the elderly has kind of been along with the technology that is present to do it?

Mr. FRANKEL. That is correct. As phone calls have gotten cheaper—some of you will remember when we used to pay 25 cents to call across the country per minute, and now it is just included in your cell phone plan, so technological progress has brought the cost of calling way, way down, has made mass calling available more readily to more people, including more scammers.

Senator BRAUN. How many VoIP providers roughly are out there? You said it is basically a small group that kind of specializes in the scam.

Mr. FRANKEL. Well, I want to be clear that there are a number of VoIP providers, and many of them are legitimate.

Senator BRAUN. Roughly how many would that be?

Mr. FRANKEL. I think there probably are a few hundred businesses that use VoIP at the core of their business. Maybe a thousand even.

Senator BRAUN. Yes.

Mr. FRANKEL. I would wager that there are a few dozen that are positioned to have their platforms used for illegal——

Senator BRAUN. That seemingly would even make it easier to remedy this.

Mr. FRANKEL. You would think so.

Senator BRAUN. I look at it kind of similar to the opioid crisis where now we know that distributors, you know, had all the data, saw something was askew, just did not do it. Here it looks like, you know, it is an issue where it should not be that difficult to flesh this out.

The next question would be: Has any third party taken an interest in actually going after these couple dozen scammers in the same way when you need help, you generally have someone there

that is going to help out the victim that has made this, you know, a mission? Is anybody out there trying to help the elderly that are getting scammed outside of the families?

Mr. FRANKEL. Well, I do not know that I can speak to that. I can tell you that within the telecommunications industry, I think we are seeing more and more and more support for identifying and highlighting and dealing with these VoIP providers that are the conduits for the——

Senator BRAUN. I think that would be wise for the telecommunications industry, because the middleman distributing drugs that were knowledgeable of it are all getting sued in some form or another.

Mr. FRANKEL. I think it is a great analogy that you have brought up.

Senator BRAUN. Yes. Have there been any civil or criminal cases filed against anybody within the telecommunications circuit, specifically the dozen or so VoIPs?

Mr. FRANKEL. One of the things that has surprised me is that when the regulators have gone after the illegal robocallers, they go after what they call the "callers," the "scammers." In fact, if you read the indictments and the other notices, they do not name who the VoIP providers are that enabled that to happen.

Now we are seeing a shift. I have just this week been talking to enforcement authorities in this town, and they do have license revocation authority. They do have injunctive authority, and I am hoping——

Senator BRAUN. They have not used it.

Mr. FRANKEL. I am hoping that we start to see that happen.

Senator BRAUN. I will finish with this: It is like many of the things I have been involved with here in a short time. It amazes me how the underlying industries have the knowledge, put up with it; it gets to a Committee hearing before anything gets done.

I would say, like I have admonished the health care industry, when it comes to fixing itself in general, the telecommunications industry and VoIP ought to be concerned, and it is surprising to me that they have not been taken to task already. That is disappointing.

Mr. FRANKEL. They are concerned, and I think we are rallying the troops.

Senator BRAUN. Thank you.

The CHAIRMAN. Thank you, Senator.

Senator SINEMA. Thank you, Chairman Collins, Ranking Member Casey, and all of our witnesses for being here today.

Robocalls are the No. 1 consumer complaint that the Arizona Attorney General receives, and more than 550 million robocalls have been placed to Arizonans in just the first 6 months of 2019.

Robocalls are more than just a nuisance, and while not every call is a scam, we must go after the criminals who use robocalls to harass seniors. For example, some criminals pose as utility bill collectors and threaten to shut off people's power in the dead of summer. In Arizona, where summer temperatures can easily top 110 degrees, that is a threat to a senior's health and well-being, and some do pay out of fear.

I also heard from Maggie, who is here today, whose elderly parents in Tucson, Arizona, were robbed of their life savings in a sweepstakes scam. Maggie's father is a 20-year veteran of the United States Air Force, living with Alzheimer's, and has lost much of what his family saved from his military pension. Their story is horrifying, but all too common, and that is why I have worked with Chairman Collins to pass the Senior Safe Act into law last year, which empowers financial institutions to identify and stop financial exploitation before families like Maggie's lose everything.

I am proud to join Chairman Collins in introducing new legislation this Congress, the Anti-Spoofing Penalties Modernization Act, that updates existing penalties for illegal spoofing that have not changed since they first became law in 2010. Our bill also helps enforcement partners by extending the statute of limitations for these violations from 2 years to 3 years.

There have been increasing reports of hospital systems getting inundated with thousands of robocalls a day, which jams their phone systems and puts lives in danger. I heard from a doctor in Scottsdale who is required to have her cell phone with her at all times. She worries that every wasted minute listening to an automated recording is a minute that is being taken from a patient or a medical emergency.

This leads me to my first question to Mr. Frankel. What could businesses and organizations, especially those that serve vulnerable populations, do to combat these scams? To what extent do you believe these types of scams that target hospitals or pretend to be from law enforcement or from IRS impact public health and safety?

Mr. FRANKEL. Well, Senator, thank you for the question. I think whether it is a hospital or it is some other agency, I mean, these are all damaging. And the robocallers are indiscriminate in who they choose to target. It is just a fishing expedition for them to see what works. They trade stories amongst each other about what the most lucrative scam is, and if it turns out the scam of the week is to target hospitals, then that is what they are going to do. It absolutely impacts the institutions, and I think that, again, as the recipients of those calls, their ability to mitigate that is—it is too far down the line to ask them to try to do that. We can make them cautious. We absolutely have to educate them. But we have to go back to the root cause.

In fact, I will tell you that I have spoken with a VoIP provider in Scottsdale who admitted to me that he was allowing 4 million calls a day onto our network from a customer of his in India, where all of those calls are spoofed. The Indian caller is claiming to be calling from the United States, and he is allowing this, and he is livid with me for calling him out on it, and he has told me he is not going to cooperate with me further, and that if I want to get more information from him, I can get a subpoena, and so, you know, now I will chase down authorities who can do that, but there is no excuse for that.

Senator SINEMA. My second question is also for you. Adam Dupuy is an assistant professor in the School of Computing Informatics and Decision Systems Engineering at Arizona State University. Experts like Adam have called for a national effort to build a detailed map of the robocall ecosystem and have raised con-

cerns about Traceback and the new SHAKEN/STIR protocols not being a silver bullet.

In your experience, do you believe there will still be gaps in how we protect people from robocalls? Are there specific challenges in rural areas that depend on older legacy telecommunications systems?

Mr. FRANKEL. Thank you for that. I do not believe that we will ever get this problem down to zero. The scammers are very clever, and we will need to have programs and systems in place that react to how they react to what we do, so it is a moving target, and we need to plan for that.

That said, I think that there absolutely are things that we can do that will dramatically reduce and limit this.

With respect to your question about rural communities, certainly with respect to SHAKEN/STIR, call authentication technology, that is a new technology. It relies on new networks in order to work, and traditionally—and we know from the rural providers that they tend to be the last to upgrade their networks, so their ability to take advantage of that new technology and offer that new technology to their customers is some long way, years away. But these robocalls, these illegal robocalls do not come into our network through rural carriers. They come into the network, as the diagram showed, way upstream from them, and if we stop them there, we will stop them for everybody, and they will not be able to reach urban dwellers, and they will not be able to reach—or they will be at least very limited in their ability to reach rural customers as well.

Senator SINEMA. Thank you.

Thank you, Madam Chairman.

The CHAIRMAN. Thank you.

Senator MCSALLY. Thank you, Madam Chairman. I really appreciate you having this really important hearing today. It is impacting so many of all of our constituents around the country. And I do want to point out Maggie Dickens, who is here today—can you raise your hand, Maggie, and say hi?-—and her story of her parents that were robbed of nearly $750,000 because of these scams, and I want to share more of her story because I think it is so important as we look at this issue.

The individuals who stole from her not only convinced them to wire the money, but trained her parents to wrap cash in magazines to send through the mail. They prepared scripts for them to read to a banking institution to legitimize the need to send these thousands of dollars internationally. They impersonated her parents over the phone to the life insurance company, allowing them to cash in her parents' life insurance policies.

When the criminals did not get answers fast enough—and I am reading your testimony—from Maggie's parents, they "sent taxicabs to my parents' home to deliver messages and try and get my parents into the cabs. Additionally, the individuals instructed my mother to open multiple credit card accounts and advance cash and buy a large number of gift cards from retail stores, all of which were sent overseas."

They are both elderly, and your father was at the beginning stages of Alzheimer's when all this happened, and he is a 20-year Air Force veteran.

As they have gone through this experience and Maggie started—as you understood what happened, you think about how many people were touched just by what I just—how many people they interacted with through this whole process. It starts with a robocall. But then there are so many other people who are on the front lines of identifying that something not right is happening here, but nobody acted.

We have had a lot of great discussion today about what more can be done. First, we have got to stop the robocall in the first place. But there were so many other indications that they were about to be robbed. What more can be done, Sheriff Sanders, what you have seen in your experience, to address this at the front lines of all these other people who were touched in the midst of this scam as their life savings were robbed? This is so tragic, and, Angela, your story is similar, but it is happening everywhere. What else can we do, Sheriff?

Mr. SANDERS. Well, the typical answer would be more police. That is not the answer here. The answer is what we are doing now. The answer is requiring the laws that are being proposed by Senator Casey to be passed so that the technological industry has some constraints and expectations, legal expectations that it has to live up to. It is everything that we are talking about. It is everything. It is family looking out for elderly relatives. It is friends looking out for elderly friends and making them aware of what we are aware of. Everyone here needs to be making this part of our daily routine and dialog when we come in contact with a senior, and they are coming at us in a technological way, but our response has to be——

Senator MCSALLY. In a human way.

Ms. De Leon-Colon, you said that veterans are more likely to be scammed. Maggie's dad was a veteran, so can you elaborate more on this? As a veteran myself, this is deeply disturbing.

Ms. DE LEON-COLON. Yes, it is because the scammers, they are going to lock onto victims that will provide a benefit to them through their schemes, so the veteran's benefits, it entices the scammers in order to obtain access to their information.

In order to add to what Sheriff Sanders said, education is a great piece. We have to educate our veterans and their families the same way that we have to educate the elderly. But it is very important that we education the community as well as their families in order to be able to identify when one of our family members, elderly or a veteran, is being targeted.

Another aspect that we have to look to veterans is because they utilize emotion, so they know that the camaraderie within the veteran community is large, so when they entice them, they tell them that they are veterans as well. They come into conversation scheming up situations where you are going to help other veterans, creating charities as well in order to help your brother, and that is how they entice veterans.

Senator MCSALLY. There is a special place in hell for people who are preying upon those who served and sacrificed for our country. We need to go after these people. But it starts with a phone call.

I have got a neighbor. She is in her 60's. She is pretty technologically savvy, and she all of a sudden is getting nonstop calls. We do not know what shifted and what list she got on, but nonstop robocalls, and the technology has got to be there to stop it. I know we have talked about it. She has gone to the provider, and they are saying, "Well, you have got to upgrade your phone if we are going to try something else on it." She does not have the ability to upgrade her phone. She cannot afford to upgrade her phone.

What else can we do, Mr. Frankel?

Mr. FRANKEL. Well, I hate to sound like a broken record, Senator——

Senator MCSALLY. I know.

Mr. FRANKEL [continuing]. but by the time the call gets to your neighbor and to her provider, it is lost in a sea of millions of other calls, many of which are legitimate, so identifying it at that point is very, very difficult for her provider. The stopping of the calls needs to move upstream to the point where that concentration of millions of illegal calls is coming into our network. That is the provider that has the ability to identify and stop the calls, and unlike the rest of the telecommunications community that is rallying and, like you, is livid about these calls, these guys are just asleep at the switch and letting it happen.

Senator MCSALLY. They need to do more. In fact, the guy there at the store said, "Well, I just ignore them when they come in." You cannot ignore hundreds of calls every day, and you are missing out on loved ones and others.

I know I am way over my time, so thank you all for your testimony, and thank you, Madam Chair.

The CHAIRMAN. Thank you very much for describing Maggie's story as well. We appreciate that.

Senator JONES. Thank you, Chairman Collins, and also, thank you, Chairman Collins, for all your leadership on this issue. It is so important. As someone who has elderly parents, one of whom still lives by her telephone, it is really important.

I want to highlight something because one of the problems I see that we have—the education, we have talked about it. Everybody has talked about it, and I want to come back. But when elderly folks get calls from someone who appears to be a legitimate law enforcement office or whatever, you can talk to them all day long. But if the sheriff calls, they are going to take that call, and recently, we had a constituent—and I think this is all important for us on this dais here—call us to tell us that they had gotten a call from Senator Jones' office checking up on their Social Security benefits, and they have to verify information about their Social Security number because they are in—we have checked and my office knew that they were about to lose their benefits if we did not get their number and help them verify that. Now, that senior was smart enough to call our office and say this is happening, so we are doing that.

We can talk about education a lot, and I agree, and I talk to my mom all the time about this. Where are our seniors, though, getting most of their information so that the education can be there? There are not that many of them out there that are watching C-SPAN today to watch this hearing. There are not many out there

that are going to always read—my mom cannot see good, so she gets something in the mail, she cannot see it.

Sheriff, Ms. Stancik, I think you can answer this better. When we are educating folks, where are they getting their information? Because it is a different generation that is not getting it all on their telephone or their iPad. They are looking at TV; they are listening to radio. Where can we do that? Where are they getting their information? I will leave it to anybody to answer that.

Mr. SANDERS. Mr. Jones, I believe one place that should be informing our seniors is places of worship. Many of our seniors attend regularly, and I think that the leaders in faith-based organizations should make this information available to our seniors.

Senator JONES. Okay. Ms. Stancik, do you want to—where was your grandmother getting her information?

Ms. STANCIK. I would say doctors' offices would be a good place. Anyplace like you said, in church, even with PSAs or other mailers that they can get, they do get a lot of mail. But things that are easy for them to understand and easy for them to read I think would help. But doctors' offices, places of worship, all those are really good places to reach our elderly.

Senator JONES. Okay. Is it television? Can the media companies help with this when they understand and know a scam, that you report a scam, can somebody—can we tell the FCC or somebody to say, for God's sakes, do some public service announcements about this? And not just do it on the nightly news because they do not always watch the nightly news. Would that help?

Mr. SANDERS. All of the above.

Senator JONES. All right. Mr. Frankel, let me followup with you real quick because technology jumps way ahead quickly, and I think that the generation—my mother's generation now and maybe mine—I am 65, and so maybe even mine—they are not always as technologically savvy. But as our population ages and my children and those in the 50 or so range, they are going to know about this a lot better. They are going to be better educated. But there is going to be something else.

What is it we have got to do to stay ahead of the game? What are we looking at in 5 years, 10 years down the road so that folks that are 50 years old now or 55 years old now, who are pretty technologically savvy and they know when they get a call from the sheriff that they are going to come arrest them because they did not pay a parking ticket, they know that that is a scam. But what is the next big thing here that we need to be looking at? How do we stay ahead of the game?

Mr. FRANKEL. Well, sometimes I say, Senator, we need to think like a robocaller or think like a scammer. First of all, the stories we have heard, the scammers are employing a broader range of technologies. It may start with a robocall today. I think as long as the telephone is around, they are going to continue to use it. We have seen scams that originate in email, so that is an ongoing threat. But I think, my prediction is that they are going to become more targeted. There is going to be more social engineering. We have got so much information about ourselves now out on the Internet that it is very easy for a scammer to go and research all the details, and now you have gone and admitted exactly how old

you are and who your parents are and so on, and they can go find all that information pretty quickly.

Senator JONES. It has been out there for a long time anyway, so that is OK. But I get what you are saying.

Mr. FRANKEL. I understand, but it is becoming more available and more detailed, and scammers are going to become more resourceful in using it to establish credibility and to perpetrate scams of larger scale, more damaging scams in a more targeted way. That is my prediction.

I also think that it is going to move to businesses, so you are going to see—we have seen it a little bit, but there are businesses that have been bilked out of hundreds of thousands of dollars and millions through wire transfer scams and things like that where people impersonate the CFO or the comptroller or the treasurer or something like that, and they can do that credibly because they have gone and gathered a lot of information on the Internet, and then they use the telephone as an entry point.

Senator JONES. Great. Well, thank you. Thank you very much. Thank you, Madam Chairman.

The CHAIRMAN. Thank you.

Senator HAWLEY. Thank you, Madam Chair. Thank you for holding this hearing on such an important topic, and thanks to all of you for being here to discuss an issue that, unfortunately, affects all of us every day.

You know, I served as the Attorney General of my State, and I can tell you that this was the top consumer complaint to my office by far, and just last year, 2018, we had nearly 50,000 complaints in the State of Missouri, 50,000 complaints of illegal telemarketing calls, and many of those came from residents who were signed up on the State's no-call list. You can imagine their incredible frustration to understand why in the world they are still getting these calls.

As Attorney General, I joined a multi-State coalition of other Attorneys General to seek ways to stop and reduce robocalls, and these fraudulent schemes are outrageous violations of privacy, I know firsthand, and frustrate and harm Missourians and Americans on a daily basis.

Like many of my colleagues here on the Committee, I was proud to cosponsor the TRACED Act, which passed the Senate in May, and I am proud to join Senator Collins on the Anti-Spoofing Penalties Modernization Act, which I hope will soon move forward, and I hope that both of these will make a real difference.

Mr. Frankel, can I just start with you? I want to come back to the topic that Senator Sinema raised about rural communities. Looking at the STIR/SHAKEN authentication technology, a lot of rural carriers still use the legacy—and you were, I think, alluding to this with Senator Sinema-—the legacy time-division multiplexing, TDM, networks rather than the voice IP technology, so am I right in thinking that the STIR/SHAKEN authentication technology cannot be used by carriers that use TDM networks? Is that right?

Mr. FRANKEL. In its present form, that is correct, Senator.

Senator HAWLEY. Can you just give us a brief description for the lay person as to why those two are not compatible, why we should care about that, why that is a problem?

Mr. FRANKEL. Well, you should not have to care about it. The industry should care about it for you. But a brief explanation, the TDM technology dates back to the late 1970's, deployed largely in the early 1980's. You know, the same reason that you cannot run modern programs on a 20-year-old computer, these protocols do not work in that old technology. It is good enough to carry telephone calls, but it is not good enough to carry all of the signatures and the encryption data that is associated with this latest STIR/SHAKEN.

Senator HAWLEY. Got it. What are some other ways, then, in your view, that we can protect rural residents and others who use carriers that rely on TDM networks? You mentioned stopping these calls up network. What are some things, what are some solutions for folks who use these networks that we can be pursuing?

Mr. FRANKEL. Well, I really do believe stopping it up network where the calls do enter our U.S. telecom system, that is the right place to stop them, and that is not dependent on all of the technology down at the customer-serving, the consumer-serving level, be it rural or otherwise. That is dependent up higher in the system where we have a small number of providers through which the bulk of these calls come. That is where they should be stopped, and the providers down there at the consumer level I think should actually be demanding of the rest of the industry upstream, saying: Do not send us this garbage. We will not accept it, and we require that you and the people upstream from you, everybody up the chain, needs to be responsible and needs to be diligent and do whatever it takes to stop those calls.

Senator HAWLEY. Are there policy steps that we could take, regulatory or otherwise, incentives that we could put in place to help stop these up network?

Mr. FRANKEL. Well, I think there is certainly encouragement that you can provide to do that. Certainly I also hear concerns from the industry. We are a very litigious society, and so, for example, providers are concerned that we are going to get in antitrust trouble if we all agree down at the customer-serving level that we will not accept this garbage from up higher. Is somebody going to accuse us of colluding to stop robocalls?

Now, I think that is ridiculous, and you are smiling, but I hear that, you know, routinely from people. We need to be very careful what steps we take because we do not want to get in that kind of trouble.

I will tell you that I went to a few having identified a couple of these providers, I called them, engaged with them via email and telephone, saying, "Please can you stop." And what I got back from two of them was threats that they were going to sue me for fraud and harassment. Can you imagine, these providers that are putting millions of calls, garbage calls, on the network every day are telling me that I am acting fraudulently and harassing them?

Senator HAWLEY. That is incredible.

Thank you, Madam Chair.

The CHAIRMAN. Thank you. That is absolutely outrageous.

Senator BLUMENTHAL. Thank you all for being here today. Thank you, Madam Chair, for having this hearing.

If this is the fifth hearing on robocalls since I have been in the U.S. Senate, it is probably the 150th. I was Attorney General of my State as well. This problem has been endemic as a consumer challenge for years and years, and the technology is there to stop these calls, correct? I do not see anyone disagreeing. It is there.

I have introduced a measure called the "ROBOCOP Act," which would require telecom companies to verify Caller ID and provide—here is the important part—free robocall-blocking technology to consumers. We have taken action in the Commerce Committee to approve a measure that is called the TRACED Act. It is on the floor of the Senate now. But it still fails to require this technology, which is there and it has been there for years, to be provided to consumers.

Is there anyone here who opposes the ROBOCOP Act? Or to put it more positively, would all of you support a measure to provide this existing technology to consumers to block robocalls? And we are not talking about public service, you know, your community is about to be flooded or there is a criminal shooter in your midst. We are talking about commercial robocalls that are done to harass and exploit seniors and the rest of us. Anybody here who opposes it? Would everyone here support it?

Mr. FRANKEL. Senator, if I may, I do not oppose the bill, but I have to tell you that the blocking technology at the terminating end of the call where it is about to be delivered to the consumer is trivially defeated by a robocaller.

Senator BLUMENTHAL. Well, with the great scientific knowledge we have—and we are celebrating the Apollo anniversary. If we can put a man on the Moon, can we defeat that kind of robocall ingenuity?

Mr. FRANKEL. That is absolutely what we have to do, but you have to recognize that for every phone call that there is a point of origination and there is a point of termination. There is the caller and the called party, and if the caller's provider is complicit in the perpetration of these illegal calls, then at the terminating end they are virtually helpless to do anything about it, so engaging the major providers to provide the best blocking technology they have is not going to work if there is somebody at the originating end that is complicit in defeating that technology.

Senator BLUMENTHAL. What would be necessary in terms of technology to block that complicity?

Mr. FRANKEL. Well, you have to hold those originating providers accountable for what they allow onto the network.

Senator BLUMENTHAL. Are suggesting that holding them accountable, holding them legally liable would be the answer?

Mr. FRANKEL. I think that would be helpful, yes.

Senator BLUMENTHAL. That should be part of the bill?

Mr. FRANKEL. I am not a law writer, but I think we should figure out, yes, how—they are so obstinate, this handful, I think there are tools that exist today that we need to fully deploy to rein them in, and to the extent that can be backstopped with legislation, I think we should be pursuing that.

Senator BLUMENTHAL. Thank you.

Thank you, Madam Chair.

The CHAIRMAN. Thank you, Senator.

Senator RICK SCOTT. Thank you, Chairman Collins and Ranking Member Casey, for doing this. Clearly, in Florida, as Senator Rubio and I will testify, both of us have had plenty of phone calls from people that have been scammed, and we have got a lot of senior citizens in our State.

Ms. De Leon-Colon, thank you for being here from the great State of Florida. What else can we be doing to just get the public—I mean, the best thing is that the public would know. I think we ought to pursue what Senator Blumenthal was talking about, what legislation we can do. But what should we be doing to get people more knowledgeable?

Ms. DE LEON-COLON. What the Postal Inspection Service is doing, we have compiled a series of public announcements that they are focused toward elderly and they are provided across the Nation, and we have actually collaborated as well with the National Center on Elder Abuse in order to prepare literature that will actually focus and speak to that senior citizen so that the information that they are receiving is good for them and is in a way that they can understand, and they are informed on how to avoid being targeted, also where to report and what to except and what the trends are as well.

We have national campaigns, National Consumer Protection Week, that we do in collaboration with the Federal Trade Commission, and we do that yearly. We go out to the post offices, and we provide talks to our customers.

We also have first-line—we have our clerks out there that have the interaction, and they usually know at the small post offices, they know their customers, and they identify—they also speak to them as well, and also they call us. They know to call us.

Education is key, and it is not just to the elderly community. It is society's responsibility, so we need to go to those churches, we need to go to those doctors, medical facilities. We need to have those social workers aware, and law enforcement has to be a part of it. It is a holistic approach.

Senator RICK SCOTT. Just take seniors in Florida as an example. What percentage of seniors in Florida do you think are aware of all the games, how they can be taken advantage of?

Ms. DE LEON-COLON. I do not have that information. I would like to provide it to you at a later time.

Senator RICK SCOTT. OK. Do you have any feel for—I mean, are people getting more knowledgeable about it?

Ms. DE LEON-COLON. I think there is, and the way I believe people are getting more knowledge on it is that we are educating their family as well, so when we go visit our elder parents, we look through the mail. Tell them to look through the mail. Sometimes you are there, we see the phone calls. They do have to have their autonomy, but it is okay. They took care of us. It is our turn to take care of them. Actually, letting society know that it is society's responsibility, it is not just the elderly's responsibility to take care of themselves, so I believe that has helped put the message out there.

Also, legislation, the cases that we are working in collaboration within the State, local, and international authorities helps as well, has helped shine a light on this issue.

Senator RICK SCOTT. Thank you.

Sheriff Sanders, what have you been able to do that has worked in your area to get—take whatever group, but seniors more knowledgeable about what is going on?

Mr. SANDERS. Community affairs, going out to the public arena in terms of senior centers. We schedule with their directors to appear and give advisories on this. We also put out public information articles about web scammers, and we also ask for suggestions as to what more we can do because all of us, if we invite comments such as you are doing today, we are collectively stronger. In my office, we ask for suggestions as to what more we can do.

Senator RICK SCOTT. Ms. Stancik, you have been trying to make people more aware because of what happened to your grandmother. First of all, my heart goes out to you. What do you think has worked the best as you have watched what is going on around the country?

Ms. STANCIK. I am not an expert. I can only speak from my grandmother's situation. I wish that there would have been more things in place to alert her. I know so many people that this has happened to now. I mentioned in my testimony I know some very close family friends who are victims of the grandparent scam, and I wish that I would have reached out to them more to explain to them the way that these criminals are reaching out to them. They lost I believe $4,000 through this scam, and they live on a fixed income, and this really hurt them.

I tell everyone I know, when I hear of a new scam, I call my parents. I tell them. I live in a very rural area, but everyone that will listen, I tell.

Senator RICK SCOTT. Thank you.

Ms. STANCIK. Thank you for that question.

Senator RICK SCOTT. Thank you, Chairman Collins.

The CHAIRMAN. Thank you very much, Senator Scott.

Senator ROSEN. Thank you for bringing this very important hearing. I know we are here on Aging, but these robocalls, these scams, they affect everyone regardless of age, and so we need to bring this probably to every committee, to the whole Senate, because it is very important.

I have to say that I have a little bit of an irony here because I was on the floor voting in the Senate last week, and I stepped away. I was waiting for an important call, so I had a call from a number I did not know. I thought that was the call, so I stepped off the floor, and I answered the phone. Well, unbeknownst to me, my Social Security number had been deactivated. I am standing off the floor of

the U.S. Senate as a Senator receiving a robocall you know, with: "If you do not press this number, you will be deactivated." I mean, the whole robot voice and everything.

Now, that is—excuse me—pretty ironic when you think about that, so—excuse me, I am suffering from a summer cold, so nobody is immune to that, not even United States Senators.

My question is—excuse me one moment. I am sorry.

Many people, especially the elderly, have plans where they have to pay for every incoming call—I really apologize, so do you think—I have had calls from constituents. This really increases their bill, so can we require cell phone companies to have some kind of mediation so that people do not have to pay for these incoming robocalls? Anyone have a comment on that?

Mr. FRANKEL. Senator, I do not speak for the industry. I am very familiar with it. It is very difficult—in fact, as I explained, it is virtually impossible for the terminating carrier, for AT&T Mobility or Verizon Wireless, T-Mobile, Sprint, to know that this is a scam call and to block it or to not charge for it or count against a minutes plan for it.

I mean, in some cases, when they do manage to block the call, the good news is it does not go through; you do not get charged for it. If they put "Scam Likely" on it and you decline the call, you will not get charged for it, but beyond that, there is not a mechanism, certainly not an automatic mechanism, and I would just tell you—I will just stop talking at this point.

Senator ROSEN. Because of my summer cold, I apologize. Thank you.

The CHAIRMAN. Thank you, and we wish you better health soon.

Senator RUBIO. Thank you. Thank you all for being here. Let me just say the numbers are startling: 26.3 billion of these type of calls in 2018. It feels like at least 5 percent of them were to me, I got to tell you, because just in the last 6 months—I just wrote some thing I remember: this robot voice telling me I am going to jail; I forgot who I owed money to on that one. There was another one saying they had stolen my Social Security number at the border—these are actually voicemails that they leave. "Somebody stole your Social Security number at the border. We need you to call us right away." Some are in a foreign language, like a recorded statement, so I do not know what those are about.

The point is I think I count last night I had 106 or 86—I forget—blocked. You know, every time when you get one of these calls, you just put it on your block list. I have more blocked numbers than I have contacts at this point, but, you know, they keep moving on these things and the like, so it is just overwhelming.

Part of this, too, is you get afraid—you cannot answer your phone for legitimate calls anymore, right? Like you pick it up, if you do not recognize it, just because it says "John Smith," it is not John Smith. You know, they have figured out a way to spoof so it is your local area code.

The purpose of this hearing in particular, I want to focus on two parts. First, Ms. De Leon-Colon, being in the Miramar office, between Broward, Palm Beach, Miami-Dade, a huge concentration of elderly citizens, and particularly in addition to that, a huge number of elderly citizens who perhaps are not fully proficient in English, making them, I think, even more vulnerable to sort of the fear, and on top of everything else, you know, senior citizens have good credit ratings, have complied with the law. The last thing they want to do is be outside of it and someone is calling them telling them, "Unless you pay us, something bad is going to happen to you."

I think you have touched on it, and maybe I missed it before I came in, but this really seems to me like something that calls for a much broader, with industry participation, public awareness, public service campaign that we have led on multiple other efforts. Everybody knows now you do not leave an animal in a locked car with the windows up—or even with the windows down, for that matter, in the middle of the summer—or at any point, for that matter. People now know you should not be eating foods that the package has been tampered with. You name it. On numerous occasions, with sudden infant death syndrome, this Nation has undertaken an effort to inform people about the dangers and the types of dangers that lie out there, and I guess it is for everybody, but most certainly knowing the intricacies of Florida, it just seems to me like this is something that is beyond just the elderly population. Oftentimes the people who spot this are their children or their caregivers, and a lot of times, the other thing I have come across is that when someone falls victim, they realize it, and there is shame associated with it, so they do not want to tell anybody about it.

That is why I think it is so important that we have a broad sort of public awareness campaign that includes everyone from retailers and others. You know, if an elderly person shows up at your point of sale and is buying—I do not know what this year's scam is. It used to be—what was it, iTunes or cards? I mean, that is suspicious, you are buying 100 iTunes cards or something, all the way to their caregivers, their children, and themselves. I really, really think that this is the kind of issue that really calls for a much broader public awareness campaign. Everyone knows these calls are coming in. I still am shocked at how many well-informed individuals fall for this for whatever reason.

I do not know if that is something any of you have had experience with, or do you think we are doing enough to inform people? I have got to tell you, most people know these calls are annoying. I am not sure how many people know the risks of the scam end of it.

Ms. DE LEON-COLON. Senator, education is key. Prevention—you prevent a crime, it is not going to be enticing for the scammers, so prevention is key, education as well, and legislation. It is a holistic approach. Educating the elderly, educating society does help. We brought this issue to light today, and you can tell word of mouth, you go, you visit your parents, you visit your grandparents, the caregivers. It has made an impact, and I think it is important to continue because scammers change their tactics. Technology evolves, and they will evolve with the times as well, so it is a continuous effort.

PSAs are very powerful. I think that also a lot of the people who have been victimized do not want to come forward because it does not seek certain structure. It happens—some of the elderly, when we have sat with them during our enforcement operations, and we speak to witnesses and victims. They come forth and say, "This was my last opportunity to leave something to my family." It is not a matter of their education. It is our responsibility and it is their opportunity to leave something behind, so education is key to prevent.

Mr. FRANKEL. Senator, if I might, I am all for education campaigns, and I think doing it through caregivers and through places like where my parents live, continuing care facilities, those are all great places to do this, and I know it is happening and I applaud it.

I would just tell you, if I were a robocaller, down the road I am going to call you, and I am going to say, "Hi. I am from the IRS. I know you have heard our announcements that we do not make phone calls and we do not collect money via gift cards, but we have got a new program, and that has changed." You say that to a million people, a few of them are going to be compelled to believe it. You are going to sound so credible: "It was my department that put that ad on television. That was 2 years ago when we produced it, but we have a new program thanks to new technology, and it is actually cheaper for you now to deal with us over the phone and to pay your tax debts via this new"——

Senator RUBIO. I am out of time, but just say that I 100 percent agree that we can tell people not to leave sugar out because the ants are going to come, like in your example, but you have still got to go after the ants. I ran out of time, but I do think it is worth—it is outside the jurisdiction of this Committee, but the idea that—one of the points you made is that there are very few legitimate entities that need the ability to make millions of calls per day, have a valid reason for using different calling numbers, and it makes no sense when they are outside of a country and their only identifier is gmail. I think that is really worth exploring further, because I think that is a great point.

The CHAIRMAN. Thank you very much. That is a reason for you to cosponsor my bill to double the penalties.

It is very clear that we need an all-of-the-above approach to this issue. We definitely need to get the technology implemented that can stop these calls and the spoofing, which I think is what causes people to answer and believe those calls, and we also need effective enforcement, law enforcement for those who have ripped off people in this country, and we need the educational campaign.

All of you have played a role in each of those areas, and I want to thank you so much for your participation today in this hearing. Each of you has really made a difference.

We are going to pursue this because when you look at the numbers, as Senator Rubio has said and as I outlined in my opening statement, it is billions of calls coming in, and I talked to a veteran in Portland, Maine, who testified at one of our previous hearings, and he said, "When I saw the IRS was calling me, I assumed that I must have missed a tax bill." Then when the next call was the Portland Police Department saying, "We have a warrant for your arrest unless you pay up your tax debt immediately," no wonder he believed that, so the spoofing is so much a part of these scams.

I want to thank the Postal Inspection Service for your enforcement, and the Justice Department. All the agencies are much more activated than ever before. The TRACED Act legislation that each of us has introduced, the Senior Safe Act, which became law last year, is making a difference, and allowing financial institutions to question these transactions without worrying about violating bank secrecy or privacy laws, so it is an all-of-the-above approach.

Our votes have started, so much as I would love to do another round of questions, we are not going to be able to. I would ask Ms. De Leon-Colon if you would leave with us some copies of the literature that you held up, because we can help distribute that. We have a Fraud Book that we put out every year, and that would be a welcome supplement to our educational issues.

Mr. FRANKEL. Most certainly, we will be glad to. Thank you.

The CHAIRMAN. Thank you.

Committee members will have until Friday, July 26th, to submit additional questions for the record, and again, I want to thank each of you for being here, for putting a human face on the problem, talking about law enforcement, the educational campaigns and technology. We need an all-of-the-above approach to put an end to scams perpetuated through robocalls that are literally costing Americans, but particularly our seniors, billions of dollars each year.

Senator CASEY. Madam Chair, thank you very much. I want to thank our witnesses. In the interest of time, I will submit a statement for the record, but I do want to thank you for the work you did today because you have helped advance the ball on this. We have got a lot more work to do at the prevention level, but also at the choke point that was discussed earlier about making sure we are doing both prevention and, frankly, prosecution and using every bit of technology to stop it.

Ms. Stancik, we are just grateful you are willing to bring your personal story. That has got to be very difficult to do, but you are helping a lot of other people by doing it, so we are grateful.

Sheriff, I will see you back home, and I will submit a statement for the record.

Senator CASEY. Thank you, Madam Chair.

The CHAIRMAN. Thank you very much.

This hearing is now adjourned. I also want to thank our staff for their hard work, too.

[Whereupon, at 11:14 a.m., the Committee was adjourned.]

APPENDIX

Prepared Witness Statements

Testimony of

Angela Stancik

before the

United States Senate

Special Committee on Aging

"Combatting Robocall Fraud: Using Telecom Advances and Law Enforcement to Stop Scammers and Protect Seniors"

July 17, 2019

Good Morning. Thank you, Chairman Collins, Ranking Member Casey, and other members of the Committee for inviting me to be here today. I am very honored.

My grandmother, Marjorie Jones was a victim of elder fraud. There are no words to express what she meant to me and my family and how much we all loved and adored her. The examples of her faith and love cannot be confined to words and she will forever be missed.

My grandmother was targeted and pursued non-stop by a ring of fraudsters. Over time, these individuals used creative and cunning tactics to gain her trust. They told her she had won a large cash prize and all she needed to do was pay taxes and fees.

I first realized my grandmother was a victim of elder fraud by the last conversation I ever had with her. Reliving that phone call is very painful for me. She explained that she needed $6,000 wired to her as soon as possible. Her forceful tone and desperation was very upsetting. I could hear the panic in her voice and she was very afraid.

This phone call set off many red flags and everyone grew extremely concerned about her financial situation. We do not know of a single time in her entire life where she ever borrowed money from an individual. My father informed me that he had wired her $8000 the week prior and he assured me he was trying to find out what was happening. He mentioned his fears that someone was scamming her, but because she was so desperate and scared, he sent her the $6000 she wanted anyway. Sadly she died less than a week later.

It pains me to talk about my grandmother's horrific death because she chose to take her own life. It is extremely hard to imagine a loved one committing suicide, but she did. Because these fraudsters preyed on her and on her good heart. Her golden years and the last chapter of her life was taken from her. It is clear to us that the circumstances that led to her death were caused by these criminals. She was robbed in every sense.

After her death we found out just how much these criminals had taken from her. We found hidden in a closet several bags full of wire receipts where she had been sending large

amounts of money overseas. My family visited these wire marketing services to talk with the clerks and discovered that they had warned her that this was not legitimate and they believed it was a scam. She continued to wire money, but use a different location.

We also discovered, not only did they drain her of all the money it took her a lifetime to save, but that she had taken out a reverse mortgage on her home and she cashed out all of her life insurance. She died with $69 in her bank account.

In the Summer of 2016 we were notified by the Department of Justice that the individuals who committed this crime against her were caught. One of them had been extradited from Costa Rica and was already in the sentencing phase for her punishment. I travelled from Houston to Charlotte to read my victim impact statement and to finally face one of the individuals who did this.

Because of that statement I was invited to speak with former Attorney General Jeff Sessions in February 2018, when he announced the Elder Fraud Sweep. Since then, I've been contacted by many Americans who are facing this exact type of scam. And I personally know 2 other close family friends that have been impacted by the "grandparent scam" and the "medical debt collection scam"

On behalf of my grandmother, Marjorie Jones, I want to thank the committee for hearing and exploring the growing and difficult problem of fraud against the elderly. We live in a fast-paced, youth-oriented society and elder issues are not high on the social agenda. But you have the ability to show great leadership by shining a light on this topic. So again, I thank you for your passion that has helped raise awareness for this issue. Thank you for recognizing that as a government, as a society and as individuals, we must increase our efforts to ensure that our seniors are protected from the criminals that prey on them. Our seniors deserve to live out their lives with dignity and honor.

Thank you.

Written Testimony of Jerry L. Sanders Jr., Sheriff
Delaware County, Pennsylvania

RE: COMBATTING ROBOCALL FRAUD: USING TELECOM ADVANCES AND LAW ENFORCEMENT TO STOP SCAMMERS AND PROTECT SENIORS

July 17, 2019

Chairman Collins, Ranking Member Casey, and members of the Committee, I am Sheriff Jerry L. Sanders Jr. and I serve as the Sheriff of Delaware County, Pennsylvania. Thank you for the opportunity to testify before the Committee about my Office's experience with scammers using robocall and spoofing technologies.

The Delaware County Sheriff's Office experiences occasional reports from citizens about receiving scam, or "robo" calls from unknown persons.

These scams vary but the most common form is the caller claims the potential victim has missed jury duty and there is a warrant for their arrest. The caller will identify themselves as a member of the Sheriff's Office, typically using a fake name. In one recent incident, the caller used the name of an actual deputy, going so far as to use the deputy's voicemail greeting as their own. If the Sheriff's Office is able to get a number from a potential victim, calling it back typically results in no answer. On occasion, someone will answer but once they realize the call is from the Sheriff's Office and we are asking legitimate questions, they typically terminate the call.

Another aspect of this is the callers often use "spoofing" technology. This is when they are able to program the actual Sheriff's Office main number to show on the potential victim's caller ID. This is often how we find out about the calls. The potential victim - in most cases people who realized something was amiss, terminates the call and calls back using the displayed number; which is the actual office number. We will tell them that this is scam - the Sheriff's Office does not call people that we have business with; that it is either done through U.S. mail, or in most cases, in-person service by a deputy. In addition, that in no circumstance would we ever ask for information over the phone and never ask for money, or any other valuable thing to avoid obligation, or arrest.

In two separate incidents that occurred over the last several months professionals were targeted. The scammers convinced two of them that they were subject to arrest for missing jury duty. In one case, they were able to get the victim to travel to a bank to withdrawal 3,000 dollars and then on to retail

establishments where she was instructed to purchase thousands of dollars in money cards, or gift cards and ended up mailing them off. The victim's husband grew suspicions and looked on the Sheriff's page on the County website and saw the scam alert but it was too late.

In the most recent case, a similar ruse was used and they advised one of the victims, a 65 year old Doctor that he was subject to arrest for not responding to a grand jury subpoena. They too had him convinced enough that they had him on the phone for approximately an hour and had coaxed him all the way to a bank in Media, Pennsylvania from his home approximately 10 miles and about 20 minutes away, to withdraw 6,000 dollars. They advised him that he should stay on the phone, not answer or communicate with anyone and to follow their instructions. His wife in the mean-time grew suspicious and tried to call him repeatedly. When she could not reach him, she called the Sheriff's Office. With that call and information she was able to provide, we were able to contact the bank and actually intercept the victim as he was parking his vehicle and thwart the execution of the scam and saved the victim thousands of dollars.

In the most recent case the victim was approached by the Chief Deputy, who was in plain clothes and arrived in an unmarked car. When the Chief first approached, the man was skeptical as to who he was, saying that he had the sheriff's office on the phone. The caller terminated the call by the time the chief took the victim's phone. Once the victim realized what had just happened, he explained that he was chiefly concerned about his medical license and that if he were to be arrested, that would be jeopardized, as well as his position as a medical director; losing sight of the fact that this elaborate ruse, with them keeping him on the phone, running him across the county, telling him to not speak to anyone, etc... was in fact just that, a ruse. He was actually intercepted a block from the courthouse, with the building in view but instead of going in to verify, he was actually going to go to the bank and withdraw the money. He then likely would have been directed to go the to a "federally authorized retailer" to purchase money, or gift cards, which he would then be instructed to give all pertinent information over the phone, and in some cases to mail them.

In the three most recent cases it is believed the scammers were able to gather personal information on the potential victims, two medical professionals and an architect beforehand, most likely from the web. This enhances the scammers ability to convince the victim that since they know much about them that the call is legitimate. This gets the victim off balance and with the threat of potential arrest and then the offer of the out - by paying a fine, they opt for that to avoid "arrest."

Frequent targets are older persons, who typically have great respect for authority and tend to be much more trusting.

These type scams circulate through the state. We will often see emails from other sheriff's offices. In response when we experience them we push out press and social media notifications to warn the public and we have a permanent alert on the county website.

Unfortunately, given the limits of manpower and resources, local law enforcement can do little to investigate these crimes to arrest. Often, trying to keep the public aware to avoid victimization is the best we can do

I was pleased to learn that Senator Casey has introduced legislation that would help train bank tellers, cashiers and others about how spot a potential scam victim and intervene to stop it. In this way, they

would serve as another line of defense – protecting our friends and neighbors from these criminals. I also think that more must be done by the telecommunications industry to stop these callers from getting through in the first place.

Thank you for the opportunity to speak before the Committee today. I look forward to answering any questions you may have.

UNITED STATES POSTAL INSPECTION SERVICE

CRIMINAL INVESTIGATIONS GROUP

Statement of Delany De Leon-Colon
Postal Inspector in Charge, Criminal Investigations Group
United States Postal Inspection Service
Before the Senate Special Committee on Aging
United States Senate
July 17, 2019

Good morning, Chairman Collins, Ranking Member Casey, and members of the Committee. Thank you for holding this hearing on stopping illegal unsolicited calls. I appreciate the opportunity to testify before this Committee on our efforts to combat fraud and to protect the American public.

My name is Delany De Leon-Colon, and I am the Inspector in Charge of the U.S. Postal Inspection Service's (Inspection Service) Criminal Investigation Group (CIG). The Postal Inspection Service is the law enforcement, prevention and security arm of the United States Postal Service. I oversee several national programs that include mail fraud, money laundering, mail theft, identity theft, violent crimes and child exploitation.

Prior to arriving at our national headquarters in Washington, D.C., I was Assistant Inspector in Charge of our Miami field office. In that role I worked closely with law enforcement partners, domestic and abroad, including authorities in Jamaica, to investigate lottery and sweepstakes fraud. I began my law enforcement career as an inspector with the Immigration and Naturalization Service (INS), and later as an agent with the U.S. Secret Service (USSS) before being appointed as a U.S. Postal Inspector in 2004.

Telephone Scams

Every day, consumers of all ages are bombarded by marketing pitches, promotions, and offers. Some are legitimate, while others are not. Most marketing pitches, especially fraudulent ones, are wrapped in language designed to appeal on an emotional level, not an intellectual one. As a law enforcement officer, I have seen over and over again how persuasive language, coupled with various forms of high-tech deception, are used to catch the attention of consumers and convince them to part with their money.

Imagine your phone rings and the voice on the other ends tells you it's your lucky day. However, you must first pay a little cash, called an "insurance fee." For some, especially older Americans, the chance to get out of debt or to leave something to their children and grandchildren has a very strong appeal. So, over the course of days, weeks, or even months, well-intentioned individuals keep sending in more money to pay the "fees and taxes," even though their "winnings" never arrive. The caller ID shows the call is coming from their local area code, or from a government agency in Washington, DC, adding authenticity in the mind of the person on the receiving end of the call. The urge to believe is overwhelming.

Once an individual has been persuaded to pay an initial fee, the scheme's operator takes the relationship to the next level, asking for yet more money, while emotionally isolating the individual from friends and family by warning them not to share their good news with loved ones until they receive their winnings. The demands for more fees are relentless, and may even include threats if the demands are not met. Because the individual believes the caller is inside the U.S., or even local, these threats are especially convincing.

What makes the recipient of these calls believe they are winners? When told exceptionally good or bad news, such as "you've won a prize," or "your grandchild has been in an accident," emotion can often override skepticism. And that is exactly what the operators of these schemes rely upon when they manipulate the consumer's caller ID display. By spoofing the phone number, the very technology designed to help consumers make informed decisions before they pick up has been turned against them. In my experience, most of the people we've interviewed were not aware that call-spoofing technology existed. By their own admission, they overcame their doubts and bought into the caller's fabulous claims because of the information displayed on their caller ID. Spoofed phone numbers were instrumental in leading the victims to believe the call was for real.

Case Example

The Inspection Service is proud to be on the front-lines investigating sweepstakes and telemarketing scams. The case in which Ms. Stancik so powerfully testified was investigated by Postal Inspectors in Charlotte, North Carolina with assistance from the Federal Bureau of Investigations (FBI), Internal Revenue Service Criminal Investigations (IRS-CI), and Homeland Security Investigations (HSI. The case was successfully prosecuted by the Fraud Section of the Department of Justice (DOJ).

The investigation focused on an offshore call center run by, Andrew Smith, a Jamaican national, and Christopher Griffin, a U.S. citizen, both living in Costa Rica at the time. The two principals, along with others under their direction, posed as representatives of the U.S. Securities and Exchange Commission (SEC) and the Federal Trade Commission (FTC). They contacted consumers in the United States, claiming they had won a substantial prize. Everyone who responded, many of whom were older adults, believed they stood to receive a significant financial reward, but they needed to make a series of up-front payments before collecting the reward. It was explained that the payments were needed to cover insurance fees, taxes and import fees.

The Costa Rican call center used a variety of means to conceal its true identity, especially call spoofing technology that made it appear the calls were placed from Washington, D.C. The understanding that these calls were coming from a long-established federal agency in the nation's capital lent considerable weight to the scam. Other internet-enabled technologies also played a role in furthering the deception. At trial, one victim testified how she was warned to keep paying the fees as the caller knew where she and her family lived. He made strategic use of images and other information that he found on the internet to reinforce his point.

In the course of their investigation, Postal Inspectors learned that payments were sent by international wire transfer directly to the call center in Costa Rica, or through the purchase of

money orders that were sent by mail or private courier. At other times, the scheme's operators hired "runners" to collect money directly from the victim, even meeting victims at their homes to collect bags of cash, which the runners, in turn, handed over to their handlers in Costa Rica.

Nine defendants were ultimately charged on various counts of Conspiracy to Commit Wire Fraud, Wire Fraud, Conspiracy to Commit Money Laundering and International Money Laundering. Eight of the defendants worked in the call center in Costa Rica, while one was charged with money laundering for his knowing participation in laundering funds from the U.S. to co-conspirators in Costa Rica. Postal Inspectors identified approximately 1,800 people living in the U.S. who collectively lost more than $10 million just in connection with this single fraudulent operation. One such person who lost a significant amount of money was Ms. Stancik's grandmother, Marjorie Jones.

With help from the Department of Justice's Office of International Affairs, the Department of State, Interpol and authorities in Costa Rica, several defendants were extradited to face charges in the United States, while others were arrested on U.S. soil. Three defendants remain fugitives and are the subject of international warrants and Interpol "Red Notices." Andrew Smith and Christopher Griffin were both convicted and, in April of this year, sentenced to 25 and 20 years in federal prison, respectively. Ms. Stancik testified on behalf of her grandmother at the sentencing of one key defendant.

The Inspection Service's Mail Fraud Program

The Inspection Service aggressively investigates frauds where there is a connection to the U.S. Mail or involves the use of a postal product or service. Examples include mass mailing fraud, lottery fraud, tech support scams, romance scams, grandparent scams and overseas boiler rooms, even when the mail is not the first point of contact. We obtain investigative leads through shared intelligence with other federal agencies, state and local law enforcement, and even from Postal Service employees who reported their concerns about an older customer they interacted with who, for example, attempted to buy money orders to send to someone they met online or over the phone.

The reach of the Inspection Service is not just limited to the United States. We understand fraud does not stop at the border, so neither do postal inspectors. The Inspection Service is one of the primary law enforcement agencies of the newly formed DOJ Transnational Elder Fraud Strike Force (DOJ Elder Fraud Strike Force). The DOJ Elder Fraud Strike Force is bringing together dedicated resources from the Inspection Service, FBI, DOJ, and other federal law enforcement agencies, as well as the private sector, to investigate transnational criminal organizations that perpetrate fraud schemes on older Americans. The Inspection Service also has inspectors working full-time in Jamaica and at EUROPOL in The Hague. We are committed to following our investigations wherever they may lead.

Prevention

Postal inspectors across the United States work every day to investigate cases and arrest the perpetrators of mail fraud, but we know an issue as broad reaching as this requires efforts on many fronts. We engage with consumers of all ages to teach them how to recognize schemes and take steps to safeguard their finances. While we work year-round to prevent fraud, each March we partner with the Federal Trade Commission (FTC) and other consumer groups for National Consumer Protection Week. We continually work to reach a wide array of consumers through presentations at town halls and community centers, events and displays in Post Office lobbies, and through social media.

The Inspection Service has launched numerous consumer protection campaigns in recent years. From 2012 until 2017, the Inspection Service produced numerous public service announcements focused on consumer fraud, which were distributed to 125 television stations covering 77 percent of the U.S. viewing audience. In 2017, we launched *Operation Protect Veterans* along with AARP to educate service members about fraud schemes that specifically target those who have served in the military. Research shows that veterans are nearly twice as likely as the general public to be victimized by fraud. According to the U.S. Census, over 9.3 million veterans are over age 65.

The Inspection Service's prevention literature offers practical advice for consumers, including how to contact phone service providers for help blocking unwanted calls. We work with academic researchers at the National Center on Elder Abuse to create messages that are meaningful to consumers of all ages, and include easy to take steps to stay safe financially. Finally, we recently upgraded our external website, *uspis.gov*, so the public can learn more about scams they may have encountered and to make it easier to report fraud.

Conclusion

Again, I want to thank the committee for holding this hearing and for allowing me to share with you the work that Postal Inspectors do to safeguard Americans from fraud. I applaud the Committee's efforts to address the issue of technologies that facilitate schemes and that give scammers an unfair advantage. Thank you.

Written Testimony of David Frankel, CEO, ZipDX LLC

17-June 2019

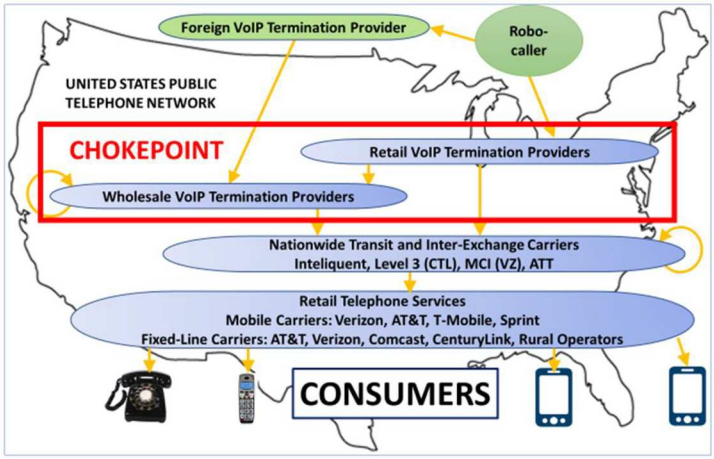
Good morning Senator Collins, Ranking Member Casey, and members of the Special Committee. I am honored to appear before you today. My name is David Frankel; I am the CEO of ZipDX LLC, a provider of specialized telecommunications applications.

While my primary business is not involved in robocalling, legal or otherwise, I became interested in the problem in 2012 and since then have devoted an increasing fraction of my professional time to addressing it.

In my remarks today, I want to share my perspective on illegal robocalls, including how they work technically and commercially, and why they persist. I will attempt to convince you that this is not an intractable problem, but it is one that requires a cooperative, focused, coordinated wide-ranging effort to address.

I have prepared a diagram that illustrates the path taken by most robocalls. The robocaller shown here, located outside the United States, buys "call termination" service from a US- or foreign-based provider. This service, typically using VoIP (Voice-Over-Internet-Protocol) allows the robocaller to initiate his calls and send his digital audio signals to the provider via the internet.

The diagram shows this near the top. The robocaller may come directly to a provider in the United States, or he may go through one or more foreign entities first. Arrangements may be "wholesale" or "retail" and the distinction is imprecise. Buyers of wholesale service often pay lower prices in exchange for higher volumes and are expected to resell the service to others. But the services are often indistinguishable.



The provider that accepts the calls from the robocaller is designated the Originating Provider. That provider typically buys (via a wholesale arrangement) terminating service from yet another provider, and ultimately the calls are sent to a national transit provider who passes the calls to the providers directly serving the called consumers. These final providers, at the bottom, are Terminating Providers – these are the providers with names familiar to consumers like T-Mobile and Verizon.

Generally, as we move down each level, the aggregate volumes increase and the per-minute prices go down. Each provider earns a small margin on the traffic. But somebody is always paying for the calls; there are commercial agreements at each link in the chain. There is no way to send a call, robo or otherwise, to a subscriber of a US-based consumer telephone service except by arrangement with an originating provider in the United States. That originating provider demands payment for the calls to cover its own costs of sending the calls downstream.

It is not difficult to become a robocaller, nor is it difficult to become an originating provider – and occasionally they are one and the same. There is software and documentation on the internet and people willing to help. You don't have to invest in any equipment, as standard computing resources can be used to process these calls and those resources can easily be rented in "the cloud."

The money involved is not large, even if the number of calls is. Charges are based on connection time after the call is answered. Since most people hang up on robocallers, connection times are very brief, averaging just a fraction of a minute.

The robocaller's approach is to place an enormous number of calls in the hope of finding a handful of respondents that will engage in his pitch. By automating the front end of the process, having a computer place the calls and do an initial screen of the target, he makes much more efficient use of his human agents who only get connected once a potential target has declared their interest.

The business models are similar, whether selling some product or service like a medical device or a timeshare condo, or referring leads for a Medicare supplement plan or a cruise line, or extorting cash by impersonating an IRS or Social Security agent. Each consummated deal will be worth $50 or $250 or $1200 in revenue to the robocaller. His biggest expense is his human agents, who with overhead might cost $20 an hour in the United States, or $40 a day overseas – and likely get paid on commission.

A typical robocaller might snag 50 victims a day, each netting him $100. Working 20 weekdays each month, he collects $100,000. He has ten agents working the phones; perhaps they cost a total of $20,000 per month.

If his agents manage to close one in four people that they talk to, he needs 200 people every day to press 1. If one in a thousand people answer his call and press 1, he'll have to make 200,000 calls daily. That will cost him roughly $400 per day or $8,000 per month

Subtracting his phone and agent expenses from his revenue, our robocaller could be making about 70 grand in profit each month. It's no wonder that this is such a popular endeavor. The originating provider serving the robocaller takes in $8,000 and pays perhaps half that to his downstream provider, so he's making $4,000 per month for allowing the robocaller onto the network.

It's been suggested that the telecom industry likes robocalls because they make money off them. This depends on who you are. For the largest providers at the bottom of our diagram, robocalls are terrible.

Costs to deal with customer complaints, implementing mitigation technologies, and overall damage to the business far outweigh the relatively miniscule revenue generated by the calls. For intermediate providers in the middle, who own and operate complex networks, it's much easier to make money on calls that average two or twenty minutes than twenty seconds. Short-duration traffic congests their network and the customers are fleeting, so they discourage it via pricing strategies and vetting whom they choose to serve.

The providers at the top of the diagram are generally small operations – a few dozen people or perhaps just one or two. Blending in robocall traffic with their other business makes for a nice supplement to their bottom line. By demanding prepayment they avoid credit risk; this is free money.

On a monthly basis, a VoIP provider that originates one hundred million robocalls could net $50,000 to $100,000 in profit. Thirty such operators would account for three billion illegal robocalls, in line with published estimates for current illegal robocall volumes. That's a big boost for these relatively small operations but peanuts in the scale of the US telecommunications business. It amounts to less than one penny per US telephone subscriber.

I want to switch gears now and talk about how we can mitigate these calls, and I'll start with an analogy to hopefully break the monotony of telephony jargon.

Imagine that we find our home infested with ants. They are in the dining room and the laundry room and the family room. Each child is assigned to ant eradication in a given room, and spends several sessions each day searching them out and removing them.

Despite our systemic efforts the problem doesn't abate, so the parents launch a rigorous investigation. Lo, they trace the ants backwards, along the baseboard into the kitchen then up the side of the island to the honey jar, where they discover a huge colony. Alarmed, they post a large sign that states "Federal law prohibits ants from congregating in and around the honey jar."

The children complain that they're falling behind in their homework because patrolling their assigned rooms for ants is consuming an ever-increasing amount of time. The parents launch further investigations and discover another ant colony at a leaking bag of sugar in the baking cupboard. Another sign goes up: "Spilled sugar is off-limits to ants." In passing, we note that the ants are failing to heed our first sign about the honey jar.

The problem continues to worsen. Finally, we hire a professional exterminator, who explains that these are a rogue strain of ants that don't comply with written instructions. He recommends adoption of a new kitchen protocol: All sugary substances must be kept in clean, sealed containers. A small investment in a sugar canister and elimination of the honey jar (which wasn't used anyway) makes a dramatic difference. The exterminator also suggests rinsing ice cream bowls and moving them promptly to the dishwasher, as he anticipates that's going to be the next sweet spot for the ants.

There is a noticeable reduction in the ant population and the children's grades are starting to improve. The patrols continue at a low level because the ants still creep in from the crawlspace and through a hole in a window screen, but the problem is now manageable.

Hopefully my analogy is not too far afield. Stopping the problem at the source – or sources – is much more effective than dealing with it once the ants or calls have dispersed. There is a cost associated with

this mitigation, but it is small compared to the alternatives. The most important measure is cost-effectiveness – for a given level of mitigation effort, how many ants or calls are we stopping? There are a finite number of sources and that's where at least some of our attention should be focused.

The best place to stop the illegal traffic is where it first enters the network. This is where it is most concentrated and its source can be identified. As the illegal calls move through the network they disperse and are comingled with other calls, making detection more difficult. Further, if a call is erroneously rejected at the point of entry, the caller is instantly made aware of that and can resolve the issue with their provider. If a call is blocked later, the cause of the block is not readily apparent to the caller and becomes more difficult to resolve.

But the first question to answer is: How do we find the source of the call? The answer should be from the Caller-ID, but takes us immediately to the problem of spoofing, which deserves a history lesson.

Caller-ID was added to the telephone network in the 1970's when digital signaling was introduced. Originating a telephone call meant creating a digital message containing both the destination phone number as well as the originating number; this message was created by the phone company serving the caller.

As digital telephony evolved over the decades, protocols were developed to allow business customers to tell their phone company which specific phone extension was originating a call. For example, if a company's published number was 202-555-1000, the company's PBX could indicate that a specific call was placed from 202-555-1234, so that the called party could know more precisely who was calling and would have a direct call-back number. The phone company would screen the supplied number to make sure it was within the range of numbers assigned to the business.

When telecom became fiercely competitive in the 1990's, business customers began using different telcos for their inbound and outbound calling. A telco providing outbound calling service didn't necessarily know which phone numbers belonged to a given customer, so rather than asking, they turned off the screening function. That was more expedient and suited the fervor of the competitive environment. "Trust but verify" became just "trust."

Now the cat was out of the bag. While legitimate businesses generally have no reason to place calls using calling numbers other than their own, the loose treatment of Caller-ID soon found nefarious applications. This predates VoIP, but VoIP made phone calls ever cheaper and more accessible and spoofing was along for the ride.

The telecom industry has only itself to blame for the spoofing epidemic, but Congress didn't help when it passed the Truth in Caller-ID Act in 2009 and chose the words "with the intent to defraud, cause harm, or wrongfully obtain anything of value." That subjective criteria leaves everybody wondering exactly what is and isn't allowable. The law should have specified only calling numbers "assigned to the caller or used with the permission of the owner." Telephone companies aren't prevented from imposing an objective criterion such as this and some do, but many do not.

Illegal robocallers go out of their way to choose originating providers that allow them to play fast and loose with Caller-ID. When a call arrives at the terminating provider, there is nothing identifying with certainty the caller or the originating provider.

However, responding to the robocall epidemic, the telecom industry now has a process to identify the source of a given call. Providers have long kept records, primarily for billing reasons, of each call handled by their networks. Working cooperatively, each provider, starting with the terminating end, searches its records for the target call and identifies the next provider in the chain that passed the call to it. The process iterates until the originating provider is reached.

Originally this process was entirely manual and was invoked by enforcement authorities issuing subpoenas to each provider in turn; that took weeks to months since there can be four or more providers involved. Now, thanks to some automation and encouragement from each other as well as the FCC, the process can be completed in days or even hours.

By tracing back selected call examples from illegal robocall campaigns, the originating provider(s) can be identified and notified and can take steps to stop the calls. Traceback learns the entire call path, so if the Originating Provider fails to act, the next provider downstream can be engaged to intervene. We don't have to trace back billions or millions of calls. We just need to trace a few examples, and we don't even need all those tracebacks to complete. One successful example can get us to the source.

When an originating provider learns that their platform is being used as a conduit for illegal robocalls, they identify the offending customer from the call examples, and examine all the traffic from that customer. That will inform a strategy for engaging with the customer to eliminate the illegal calls. The provider may also impose network-level constraints, which can include: throttling the rate at which the customer can initiate calls, restricting the number of concurrent calls; and screening the caller-ID value(s) available for the customer's use. These same constraints can and should be applied to all new customers as well. The provider may decide that discontinuance of service is appropriate, especially if violations are on-going. New and existing overseas customers warrant additional scrutiny. Identities of on-going offenders are published; other providers may elect to do extra screening of their calls.

If the Originating Provider fails to mitigate the illegal calls, downstream providers (which are receiving the calls from the Originating Provider) will be wary of continuing to accept that provider's traffic. A downstream provider will notify an offending Originating Provider of terms-of-service and/or acceptable-use-policy violations (which generally prohibit the sending of illegal calls, and often have even more rigorous restrictions). If the traffic continues, the downstream provider will act according to the terms of its contract with the Originating Provider, which can include network constraints like those mentioned above, as well as financial penalties and, in cases where the violations are on-going, termination of service.

Providers that really care about the robocall problem are revising their contracts to insist that their upstream partners cooperate in the fight against illegal robocalls and are prioritizing those revisions to those behaving most problematically.

Every self-respecting US-based telecommunications provider should be contributing to addressing the problem of illegal robocalls. That means participating in traceback efforts. But it also means being prudent about who gets what kind of access to the US telephone network. Very few legitimate entities need the ability to make millions of calls per day. Very few legitimate entities have a valid reason for using a different calling phone number for each call they place. It makes no sense for somebody in India, identified only by a gmail address, to be placing huge numbers of calls that look like they are originating from all over the USA.

US-based providers that allow that to happen are the root cause of our illegal robocall problem.

In closing, I will tell you that efforts to authenticate calls, to educate consumers and provide them with blocking apps, to implement analytics and labeling solutions that warn of bad calls, and to allow legitimate volume callers to rise above the sea of garbage are all good things to do. But I promise you that the most immediate and effective mitigation approach which can rise to the scale necessary to address our current problem rests with the handful of US-based originating providers that are letting these calls onto the network to begin with.

I welcome your questions.

Statements for the Record

Closing Remarks
Senator Robert P. Casey, Jr., Ranking Member
July 17, 2019

Thank you, Chairman Collins, for holding this hearing today.

As we learned today, scammers are still using illegal robocalls to pick the pockets of our aging loved ones. We also heard about the devastating impact these calls can have on seniors and their families. We cannot sit back and let this continue. It is our sacred duty to step in. This is why we must re-double our efforts to make sure that older adults are made aware of potential scams before they send money to these con artists. We must also continue our efforts to stop these con artists from ever connecting with consumers. Our nation's seniors are depending on us.

I look forward to continuing the work with you, Senator Collins, on this important issue, and hope that we can find some way put a stop to this once and for all.

Thank you.

ELECTRONIC TRANSACTIONS ASSOCIATION
1620 L Street NW, Suite 1020
Washington, DC 20036
202.828.2635
electran.org

July 17, 2019

The Honorable Susan Collins
Chairwoman
Special Committee on Aging
United States Senate
Washington, DC 20515

The Honorable Bob Casey
Ranking Member
Special Committee on Aging
United States Senate
Washington, DC 20515

Dear Chairwoman Collins and Ranking Member Casey:

The Electronic Transactions Association (ETA) submits these comments ahead of the Senate Special Committee on Aging hearing, titled *Combatting Robocall Fraud: Using Telecom Advances and Law Enforcement to Stop Scammers and Protect Seniors.*

ETA is the leading trade association for the payments industry, representing over 500 companies that offer electronic transaction processing products and services; its membership spans the breadth of the payments industry to include independent sales organizations, payments networks, financial institutions, transaction processors, mobile payments products and services, payments technologies, equipment suppliers, and online small business lenders.

We share the Committee's concern about bad actors who intentionally flout laws or mask their identity and location are a nuisance, or even worst, predatory for many consumers. Efforts made to detect and eliminate these calls are important for consumer protection and to instill confidence about who is calling.

However, it is imperative lawmakers recognize the difference between actual unwanted telemarketing calls, where an unknown merchant is attempting to sell to a consumer, and purely informational calls involving communication between businesses and their existing customers.

This distinction is important because ETA companies are not telemarketers - but financial services companies who have, or service, a business relationship with a customer. ETA companies either have a direct relationship with an individual consumer or communicate with existing customers on behalf of financial institutions with which they are associated. Protecting their customers' personal data and financial information is paramount.

The lack of modernizing the Telephone Consumer Protection Act (TCPA) is unfortunately resulting in significant harm to consumers, particularly in the payments industry, by hampering legitimate businesses from contacting their customers using the most efficient technology to provide them with information that consumers deserve to know and know promptly. ETA member companies seek to communicate with consumers to prevent fraudulent use of their accounts by criminals and provide updates about their accounts.

ETA supports many of the efforts to target and eliminate unlawful calls in order to distill these communication channels so that customers can trust and receive the calls about their personal financial information. We look forward to working with lawmakers, regulators, and key stakeholders to further strengthen the TCPA so that consumers get the information they want and deserve from the companies with which they do business.

We appreciate your leadership on this important issue and for convening this hearing. If you have any questions, please feel free to contact me directly at stalbott@electran.org.

eta ELECTRONIC TRANSACTIONS ASSOCIATION
1620 L Street NW, Suite 1020
Washington, DC 20036
202.828.2635
electran.org

Sincerely,

Scott Talbott
Senior Vice President of Government Affairs
Electronic Transactions Association