## Opening Statement Senator Susan M. Collins "Combatting Robocall Fraud: Using Telecom Advances and Law Enforcement to Stop Scammers and Protect Seniors" July 17, 2019

\*\*\*

Good morning. Protecting American seniors from scammers who seek to defraud them is a central goal of this Committee. In the past six 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 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 American 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's 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 perpetrate their schemes. Today, we will focus on a practice called "spoofing," which 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 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 one 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 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 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 illegal robocalls from foreign call centers closer to their source before they can reach American consumers. Today, we will learn about new network level approaches with the potential to ultimately stop robocall spoofing fraud altogether.

Beyond the technology — and we'll 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.