Opening Statement
Senator Susan M. Collins
Special Committee on Aging
October 21, 2015
Computer Scam Hearing
"Virtual Victims: When Computer Tech Support Becomes a Scam"

Good afternoon. Today the Aging Committee is continuing its focus on scams targeting our seniors. Our Fraud Hotline recently was contacted by a senior who reported that he had received a troubling call from a man who claimed to be a Microsoft support technician. This so-called "tech support representative" told the senior that his computer had been hacked and was about

to crash.

Understandably concerned, the senior followed instructions to log on to his computer and provided the caller with information that would enable him supposedly to fix the technical problem. By providing the caller with this information, he inadvertently gave the scammer remote access to his computer. In addition, the con artist was successful in convincing him to provide his credit card number to cover a $300 fee to "fix" the computer problem.

When the con artist called this senior back a few days later to ask for more money for supposed computer updates, he realized he had been scammed.

Over the past year, the Committee's Fraud Hotline has received more than 70 complaints about this scam, with the majority of calls occurring within the past three months. As our witnesses will tell us today, the incidence of these scams is increasing dramatically. In fact, Microsoft estimates that approximately three million Americans fall victim to technical support scams

annually.

In another far-too-prevalent version of this scam, the con artist uses malware or spyware to actually infect the computer with a virus so that its user is locked out. Not surprisingly, the scammer will then charge a fee of several hundred dollars to rid that computer of the implanted virus.

In yet another variation, seniors have been offered a "senior citizen discount" if they are on a fixed income and cannot afford the initial price cited by the scammer.

According to Microsoft, these computer tech support scams cost Americans an estimated $1.5 billion a year.

But even more chilling than the enormous amounts of money that criminals are stealing through this scam is the massive scope of personal and financial information to which these con artists have potentially gained access. By breaking into a victim's computer, a thief could gain access to information such as bank account and credit card numbers, passwords to investment accounts, Social Security numbers, and other personal information that could enable criminals to continue to steal from their victims.

Today's hearing will examine these troubling computer scams; efforts that could help prevent Americans, and seniors in particular, from falling victim; and efforts being made by law enforcement and the tech industry to stop these scams and to prosecute the criminals that perpetrate them.

I am pleased to welcome Mr. Frank Schiller of Peaks Island, Maine, to our hearing today. Unfortunately, Mr. Schiller is far too familiar with this computer tech scam, and will share with us

how a 2013 call led to his losing more than $1,400

to a con artist.

Putting a stop to the multitude of ruthless scams that target seniors is among the Committee's top priorities. To date this year, the Fraud Hotline has received almost 1,000 calls reporting on nearly 30 different scams, including the computer tech scam. It is my hope that hearings like the one we are holding today will help shed light on these scams, alert seniors, and

provide a catalyst for law enforcement to aggressively prosecute scammers who deliberately prey upon seniors.

I look forward to hearing from our witnesses.