S. HRG. 114–855

VIRTUAL VICTIMS: WHEN COMPUTER TECH SUPPORT BECOMES A SCAM

HEARING

BEFORE THE

SPECIAL COMMITTEE ON AGING

UNITED STATES SENATE

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

WASHINGTON, DC

OCTOBER 21, 2015

Serial No. 114–15

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

48–532 PDF WASHINGTON : 2022

SPECIAL COMMITTEE ON AGING

SUSAN M. COLLINS, Maine, *Chairman*

ORRIN G. HATCH, Utah
MARK KIRK, Illinois
JEFF FLAKE, Arizona
TIM SCOTT, South Carolina
BOB CORKER, Tennessee
DEAN HELLER, Nevada
TOM COTTON, Arkansas
DAVID PERDUE, Georgia
THOM TILLIS, North Carolina
BEN SASSE, Nebraska

CLAIRE MCCASKILL, Missouri
BILL NELSON, Florida
ROBERT P. CASEY, JR., Pennsylvania
SHELDON WHITEHOUSE, Rhode Island
KIRSTEN E. GILLIBRAND, New York
RICHARD BLUMENTHAL, Connecticut
JOE DONNELLY, Indiana
ELIZABETH WARREN, Massachusetts
TIM KAINE, Virginia

PRISCILLA HANLEY, *Majority Staff Director*
DERRON PARKS, *Minority Staff Director*

C O N T E N T S

VIRTUAL VICTIMS: WHEN COMPUTER TECH SUPPORT BECOMES A SCAM

WEDNESDAY, OCTOBER 21, 2015

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

The Committee met, pursuant to notice, at 2:30 p.m., Room 562, Dirksen Senate Office Building, Hon. Susan M. Collins, Chairman of the Committee, presiding.

Present: Senators Collins, Cotton, Tillis, Sasse, McCaskill, Nelson, Donnelly, Blumenthal, and Kaine.

OPENING STATEMENT OF SENATOR SUSAN M. COLLINS, CHAIRMAN

The CHAIRMAN. The Committee will come to order.

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 onto 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, the senior inadvertently gave the scammer remote access to his computer. In addition, the con artist successfully convinced him to provide his credit card number to cover the $300 fee to fix the computer problem.

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

Over the past year, our Committee's Fraud Hotline has received more than 70 complaints about this kind of scam, with the majority of calls occurring within the past three months. As our witnesses today will attest, 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 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 amount of money that criminals are stealing through these scams 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 our seniors, in particular, from falling victim to them, and efforts being made by Federal agencies and law enforcement and the tech industry to stop these scams and to prosecute the criminals who perpetrate them.

I am very pleased to welcome Frank Schiller of Peaks Island, Maine, to our hearing today. Unfortunately, Mr. Schiller is far too familiar with this type of computer tech scam and he has graciously agreed to share his experience with us about how a call led to his loss of more than $1,400 to a con artist.

Putting a stop to the multitude of ruthless and endless scams that target our seniors is among our Committee's top priorities. To date, this year alone, our Fraud Hotline has received almost a thousand calls reporting on nearly 30 different scams, including this scam that we are examining today. It seems the inventiveness of con artists is endless and they will constantly evolve and come up with variations on scams and brand new ones to target our seniors.

It is my hope that the hearings that we are holding will help shed light on these scams, alert and educate our seniors, and prompt law enforcement to more aggressively go after and prosecute scammers who deliberately prey upon seniors.

I look forward to hearing from our panel of witnesses today, and I am now pleased to call on our Ranking Member, Senator McCaskill.

OPENING STATEMENT OF SENATOR CLAIRE MCCASKILL, RANKING MEMBER

Senator MCCASKILL. Thank you, Chairman Collins.

Today's hearing highlights the latest scam preying on our Nation's seniors, the tech support scam, but when you think about it, these scams have been around for ages. They are confidence scams, pure and simple, and if there is one thing many seniors are not confident about, it is technology.

It makes perfect sense that these fraudsters would cling to a senior's insecurity about technology to swoop in under the guise of assistance. Not only do these scammers charge for their, "services," they also get access to personal data and financial information that could potentially be used to further other crimes. We are all very familiar with the dangers that can occur when identifying information gets into the wrong hands.

Technology scams are on the rise, so much so that the Federal Trade Commission has now turned them into their own category, and fighting them will not be easy. On the criminal side, you have anonymous actors who can work from anywhere with a computer and Internet access, and they can find victims, especially seniors, who are not very adept at understanding what is actually happening on their computers.

What can be done here? Consumer education helps, for sure, as does more robust law enforcement against scammers. However, there are a variety of consumer education organizations and a number of law enforcement entities. Often, what is the most disconcerting in these cases is they do not talk to each other and share what is working and what is not working. A general lack of collaboration makes it much more likely for criminals to succeed in defrauding victims and much more likely that a victim will not even recognize that he or she is being scammed.

In Southern Missouri, however, leaders from many of these groups have decided to come together to fight fraud. In 2013, Legal Services of Southern Missouri brought together local law enforcement, the Federal Bureau of Investigation, the Missouri Attorney General's Office, the U.S. Postal Inspector, and the Better Business Bureau to create the Consumer Fraud Task Force of Southern Missouri. This group meets at least quarterly and shares information with each other and the public in an effort to stem the tide of these scams. I am pleased that we are joined today by Lew Polivick from the Legal Services of Southern Missouri to talk about this effort as well as the scam schools his group has set up to partner with senior groups to teach seniors about new scams and ways to protect themselves.

I am eager to hear from both government and industry witnesses today to get a sense of what we can do in Congress to help fix these problems.

Once again, I want to thank our Chairman for calling this hearing and to our witnesses for joining us to discuss this problem today. I look forward to hearing your testimony.

The CHAIRMAN. Thank you very much.

Before turning to our witnesses, I just want to welcome the other Committee members who are here today, Senator Tillis, Senator Cotton, Senator Kaine, and the former Chairman of this Committee, Senator Nelson. Thank you all for being here.

Senator NELSON. Madam Chairman, you are continuing the tradition of this Committee in the way of really going after the issue and I appreciate you bringing it up. How many of these scams have we heard over the course of the last three years?

The CHAIRMAN. An endless number.

Senator NELSON. Just another one happened the other day in Florida. A woman who had lost her husband suddenly had the phone call she had won $100,000 in the lottery, that her late husband had purchased a ticket that she did not know about. That was the scam, and of course, she started paying, so thank you for doing this.

The CHAIRMAN. That is a truly cruel——

Senator NELSON. By the way, there are a bunch of our bills out here.

The CHAIRMAN. Yes.

Senator NELSON. We ought to get the leadership to combine the bills and bring them to the floor.

The CHAIRMAN. Hear, hear. I certainly agree with that, as well.

We are now going to turn to our panel of witnesses. As I said, I am delighted to welcome Frank Schiller from Peaks Island, Maine. To get here, understand that Mr. Schiller has to take a ferry first from the island to Portland and then fly to Washington. He has made an extra effort to be here today and I very much appreciate his willingness to share his personal experience in dealing with tech support con artists.

Next, we will hear from Lois Greisman, who has testified before us previously. She is the Associate Director of the Division of Marketing Practices of the Bureau of Consumer Protection at the Federal Trade Commission. The FTC is the lead civil law enforcement agency combatting these scams and also in charge of educating consumers.

We will then hear from David Finn, the Executive Director of the Digital Crimes Unit at Microsoft Corporation. He is married to someone who graduated from a fine Maine college, Bowdoin College, so we know his testimony will be excellent today.

He will talk about the extensive work that Microsoft is doing, both on its own and in collaboration with law enforcement, to combat these scams, and finally, we will hear, as our Ranking Member has already indicated, from Lew Polivick, the Deputy Director of Legal Services of Southern Missouri.

Senator McCaskill, I think you introduced him in your opening statement. If you want to add anything now, you are welcome to do so.

Senator MCCASKILL. I am just—I am proud of legal services generally. You all are woefully understaffed and underpaid throughout this country. There is never going to be justice for all unless everyone has access to legal services, and we are falling way short of the mark in this country, and your organization is doing the very best it can to keep up with an absolutely unmet demand of legal help among our Nation's less fortunate, and I just am a big fan of people who choose your work as their life's work, and thank you so much for being here.

Mr. POLIVICK. Thank you.

The CHAIRMAN. Thank you.

Mr. Schiller, please begin.

STATEMENT OF FRANK SCHILLER, COMPUTER TECH SCAM VICTIM

Mr. SCHILLER. Good afternoon, Chairman Collins, Ranking Member McCaskill, and distinguished members of the Committee. I am Frank Schiller. I am from Peaks Island, Maine, and I appreciate the opportunity very much to be here today, albeit perhaps as the distinguished dummy, to share my story as a victim of a computer scam.

While the whole episode was and is extremely embarrassing, I want to share my story with you and others today out of my concern that these criminals are still preying upon seniors and others. These people need to be stopped and their calls need to be ignored.

As a short summary of my circumstances, on October 1 of 2013, I received a call at home from somebody calling himself "Brad." He said he worked for somebody calling themselves the Kavish Techno Software Company. He said that they had a contract with Microsoft, or some probable company. He claimed that they had identified some reports from Microsoft, many, many problems with my computer's operations. He gave me a 32-item alpha-numeric code. He said if I wrote it down, he could verify my problems and further convince me that his concerns about computer problems were legitimate if I went on my computer.

I did write it down. I went on the computer. I followed his instructions, very few of them, very simple, and sure enough, what it showed was my computer's ID, its IP address. I am not sure how he got that. I was kind of amazed, and he said, well, now let me show you this. A few more instructions, and my computer screen began to scroll, pages and pages and pages of small groups of numbers. He said that was machine code, that it was from programs that were cluttering up the computer which were interfering with its operations.

How he had known my name—the call had been to, "Is this Frank?"—how he had known my phone number, how he had known my computer ID or IPA, I have no idea, but his ability to identify those things and to walk through that computer as easily as we go through our front doors was impressive, so I continued.

He said, okay, he had software to clean the computer up and to stop those malicious files. He gave me several options. One was $349. For $79 more, you could get two years additional. I said, okay, I could pay for it with Visa. He said, no, they could not accept Visa because they had to work through the Central Bank of India and Visa would not authorize payment to there, so I would have to authorize Visa directly. I was still suspicious enough to stay mute about that I had a cell phone, and said, well, I would have to get off the phone with him and call him back if he could give me a phone number. He did, with an area code of 1–90-something or other, which is in my material.

I talked to Visa. I authorized the payment. I hung up, called back, got some very ruff person, not at all like a professional at a company, I thought. He referred me back to Brad, and the process was cleared. I got a couple of additional programs for my computer. That was the end of that and Brad.

I ran those programs and it did not seem to do anything. I mean, it did not hurt anything. It did not seem to help anything. It did not do anything.

I found a support folder on my desktop at the time that had a contact file in it and it had two receipts in there from Visa, including transaction bank numbers, which are in the material I have sent with my complaints.

Then it was quiet until December 16th, nine days before Christmas, whatever. I got another call from Brad. He said that his contract with Microsoft had been canceled and therefore, he had to refund the money that they had charged me for those programs. Fine. Send me a check, I said. He said ″well, no, no, no. We cannot do that. We have to process your refund the same way that you made a payment. Again, Visa was not going to allow a transaction

from the First Bank of India. Oh, well, I am sorry. The only thing we can do is transfer it into your checking account.″ Well, this is where I get dumber.

It was right before Christmas, you know. You can always find things, people that need things right before Christmas. Okay. I gave him my account number, my routing number. He said, look, I do this every day, day in, day out. I can put this right in for you, press a few keys for me here and it will get it done. Well, what I did was gave him control of my keyboard.

The next thing that popped up was a Western Union transfer box. It came up. It flashed very quickly, miniaturized to the size of a bottle cap. In the process, I noted this $980 figure plug in. I said, well, what is that? Oh, well, I have to bundle a few transfer requests in one. Do not worry. That was done, gone.

The next day, I discovered the $980 had been withdrawn from my checking account. I have got it in my testimony, but I complained. I froze the account. I complained to the local police department. I e-mailed a complaint to Western Union. I filed—I closed the checking account. I filed formal grievances with the Maine Attorney General's Office, the State Police Computer Crimes Unit, the Federal Trade Commission. I got a very nice piece of correspondence back from the Federal Trade Commission giving me a complaint number and a counselor number in case I needed to get more upset, or not.

The next day, after I had closed my bank account and whatever, Brad called back, very upset. He wanted access to my computer. Well, no, it did not work that way. I was not going to do that again. They called me probably three times a week for the next couple months. You know, it is why they invented caller ID, but even then, it comes up "unknown." You do not quite know who is calling. You do not want to never answer the phone, but it makes you feel different about answering your own telephoned, and they vacillated between very courteous—we are sorry, there had been a mistake, if you let us on your computer, we will fix it—to very insistent—you need to get on your computer now. I am not going there.

I think it is important that people know. I worked in assisted living with elderly people. I used to give little workshops to people. Do not trust people on the phone. Never give your checking account information to anybody. Do not ever do that. Well, I did, and it was a sequence of circumstances. I was not trying to be sold something. They were trying to give me money. You know, the timing in mid-December was pretty good from their perspective. His knowledge of how my computer worked, where it would go, what it would do was beyond anything I had any imagination of.

I realize that chances of financial recovery are near zero, but I am here today to share that story hoping that it helps other people from falling into the same process, the same scam, that it helps you in your work, that it helps these agents and agencies in their work, honestly, to shut this down. I mean, there is no reason, with all the technological capacity we have on our side, that they should be making thousands of phone calls a week to thousands of people with this just terribly bogus information, just stealing them blind, and it does not do anybody any good. I mean, we have got natural disasters. We have got crises to deal with. We do not need to be

giving it to some "Brad" who I am sure is not helping out his family, neighbors, and others that need help.

I thank you for the opportunity to be here, and when we get to it, would be glad to answer any questions you have.

The CHAIRMAN. Thank you very much, Mr. Schiller, for your willingness to come forward and share your personal experience—very unfortunate personal experience.

Ms. Greisman.

Mr. SCHILLER. It has happened to a lot of us.

The CHAIRMAN. It does.

STATEMENT OF LOIS GREISMAN, ASSOCIATE DIRECTOR, DIVISION OF MARKETING PRACTICES, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION

Ms. GREISMAN. Thank you. Good afternoon, Chairman Collins, Ranking Member McCaskill, and members of the Committee. I am delighted to appear before you today to discuss the FTC's work to fight tech support scams, which the FTC's consumer complaint data indicates may have a disproportionate effect on older consumers.

I will comment briefly on the nature on these scams, the FTC's aggressive law enforcement efforts to shut down this kind of illegal conduct, and then I will talk about our outreach and educational initiatives.

As Mr. Schiller artfully described and as you have alluded to, tech support scammers use a variety of means to lure consumers into their traps and extract millions of dollars. They may place cold calls, telling consumers their computer is infected and in dire need of repair, as has happened in his case. I too, have received such calls. Scammers also may place pop-up ads offering free antivirus scans or enticing consumers with software promising to speed computer performance. Further, scammers may place ads with search engines so that consumers who truly are in need of assistance reach out directly to them.

Whatever the method, the deception is plain. Scammers impersonate a trusted name, such as Microsoft, Facebook, Symantec. They falsely State the computer is infected, often gaining remote access and displaying utility programs that to an untrained eye do support the scammers' lies about infection and the risk the computer will crash. The scammers then seal the deal, claiming they can fix the problem for maybe less than $100 or several hundreds of dollars. Overall, consumers have lost well upwards of $100 million to scammers for repairs they did not need, and those people who actually were in search of true genuine technical support were not aided.

In late 2012, the FTC initiated a major crackdown, suing a number of tech support scammers located in the United States and in India. Working with several international partners, we obtained solid orders that prohibit the misrepresentations we challenged. Just late last year, we filed yet an additional three cases against tech support scams, one of which again involved a call center operating in India. That case settled. The other two remain in litigation.

I assure you, we will continue to identify and sue tech support scammers in the U.S. and abroad, working with Microsoft and with

other industry partners, but as the testimony indicates, enforcing judgments against defendants located offshore presents a real challenge.

Working with U.S. industry members and our colleagues from Canada and the U.K., we have had a series of meetings with people in India, with authorities as well as representatives from Indian call centers and consumer groups, to develop an action plan to tackle telemarketing fraud from Indian call centers. We are not going to pretend we found a silver bullet, but we have laid a foundation from which we will seek both to encourage and support Indian law enforcement against illegal telemarketers, and I am also very encouraged that so many of our international partners are equally committed to combatting tech support scams.

Education and industry outreach are indispensable complements to our law enforcement work. "Pass It On," which I will hold up, and I hope each of your offices has taken a close look at, is really our signature education effort aimed at active older seniors. The goal is to encourage seniors to share critical information about issues such as imposter fraud with families and friends. Blog posts and videos on the FTC site also spread the word about tech support scams, and our collaborative work with the AARP Foundation, through which it provides one-on-one peer counseling, is aimed at making it less likely a senior who was victimized once will be duped a second time.

One final point. From January through August of this year, we received nearly 24,000 discrete complaints about tech support scams, and nearly half of them were from consumers aged 60 or older. I cannot over-emphasize the value of these complaints to the more than 2,100 law enforcers in the United States and abroad who access these complaints through the Sentinel data base. While it is not at all possible, unfortunately, to assist each consumer, we do mine the complaints, find commonality, such as company names, software names, phone numbers, billing descriptors, all of which we use to identify targets and build cases. In some cases, we do reach out directly to the complainant for direct assistance by way of a declaration or testimony in court.

I fully realize there are many reasons consumers do not file a complaint, and in all too many instances may not even know the tech support they received was a scam. Nonetheless, we urge all who think they see such a scam or may have fallen victim to one of them to file a complaint at FTC.gov.

I thank you and look forward to your questions.

The CHAIRMAN. Thank you for your testimony.

Mr. Finn.

STATEMENT OF DAVID FINN, ASSOCIATE GENERAL COUNSEL AND EXECUTIVE DIRECTOR, DIGITAL CRIMES UNIT, MICROSOFT CORPORATION

Mr. FINN. Thank you, Chairman Collins and Ranking Member McCaskill and members of the Committee, for inviting me to testify today. My name is David Finn. I am Associate General Counsel and Executive Director of the Microsoft Digital Crimes Unit.

My testimony focuses on technical support scams, the largest ongoing consumer fraud perpetrated in America today, victimizing 3.3

million consumers a year at an annual cost of $1.5 billion. This translates to a victim nearly every 10 seconds, with an average loss of $454 per consumer.

Since May 2014, Microsoft alone has received over 180,000 complaints about tech scams. We know these complaints are merely the tip of the iceberg. Customers of other software companies are also being victimized, and many victims are not even aware they have been scammed, but this is not a scam that can be described in just statistics and dollars lost. Behind every scam is the face of someone like Mr. Schiller, a neighbor, a friend, a family member, or a senior citizen who trusted in someone to take care of a seemingly serious problem and had that trust abused as their pockets were being picked.

In an effort to persuade seniors—to protect seniors from technical support scams, our Digital Crimes Unit has a team of attorneys, investigators, forensic analysts, and business professionals collecting information from customer-generated leads, using big data analytics and working with the FTC, the FBI, State attorneys general, and others in law enforcement.

Regardless of how the scammers initially make contact, the key for them is to get potential victims on the telephone. Our investigators have seen firsthand how the scammers bamboozle consumers. Fake support agents typically take control of the victim's computer and pop up fake warnings, saying viruses have infected your computer, unwanted people are trying to steal your information, foreign agents and Russian hackers have taken over your machine, all a complete and utter fabrication by the scammers. Having raised consumers' fears, the fraudsters then typically sell an unneeded service to fix a nonexistent problem.

Microsoft is pursuing criminals who prey on consumers, but there is a limit to what one company or what one organization alone can accomplish. In the wake of new and rising scams, the State attorneys general have become very active. Their offices are also seeing an explosion in the number of complaints. We are eager to work more closely with State AGs on both consumer protection and criminal enforcement actions, perhaps even through a multi-State action, to deter and bring to justice these criminals. Such a public-private effort combines the technical expertise necessary to investigate these cases with the leadership, legal authority, and regulatory might that State AGs can bring to the problem.

Microsoft has also worked to support the FBI and the FTC to put these fraudsters out of business. Since 2012, as you just heard, the FTC has brought a number of cases targeting technical support scams. We provided evidence and sworn testimony in many of those cases and helped the Commission staff with technical details. We have also worked with the FTC to reach call centers abroad, where many of these criminal entities are located, and last month participated in a call center fraud roundtable which included Indian and U.S. law enforcement in New Delhi, India.

Microsoft is also partnering with AARP to develop a series of scam jams focusing on online safety for seniors, and we continue these education efforts, for example, by hosting senior groups at our Cyber Crime Center in Redmond, Washington, and running

awareness workshops for seniors in our retail stores across the country.

To conclude, this is not a State or a Federal problem, but both. It is not a public sector or a private sector problem. It is both. While I have outlined the challenge I face, let me also suggest a solution: aggressive and unrelenting enforcement of State and Federal criminal and consumer protection laws that bridge law enforcement agencies and cross jurisdictional and international boundaries. While education is also an important part of any response, criminals will only stop when their greed is checked with concrete consequences, and that includes prosecution, conviction, and, where appropriate, imprisonment of the most egregious offenders.

Microsoft is committed to protecting our seniors and other computer users around the country and to working with all stakeholders to achieve our common goals.

Thank you for allowing me to be here today, and above all, thank you for drawing attention to the challenge ahead of us. I look forward to answering your questions.

The CHAIRMAN. Thank you for your testimony.

Mr. Polivick.

STATEMENT OF LEW POLIVICK, DEPUTY DIRECTOR, LEGAL SERVICES OF SOUTHERN MISSOURI

Mr. POLIVICK. Thank you, Chairman Collins, and I thank Senator McCaskill for inviting me to speak here today and before this Committee.

From the point of view of a legal aid program, addressing these scams, it has to be done through education of our clients. Once the scammers have got a hold of their money, they are not going to get it back and there is nothing we can do to get it back from them. We can try to help them correct their credit reports. We can ask them to stop credit charges on cards, that sort of thing, but the money is gone, and these people cannot afford this. You know, they are living—our clients are at 125 percent of the poverty level or below. Many are senior citizens, are on fixed incomes, and they are the ones that can least afford this type of fraud.

To that end, our program in 2013 established a Consumer Fraud Task Force of Southern Missouri, and with that, we have partnered with the Federal Trade Commission, the Missouri Attorney General's Office, the FBI, the U.S. Postal Inspector, Better Business Bureau, local prosecuting attorneys and police departments, to get the word out about these scams, to meet quarterly to find out what new is going on, what efforts are being made to address these scams, and to get the word out to our clients and the general public.

Usually, this is done through press releases. We also have partnered with Springfield news station KY3, who have established a "Scam of the Week" segment of their news show-—that is how bad it has gotten, they have a Scam of the Week—to get the word out of what is going on and to educate people not to deal with these scam artists.

We do outreach programs through what we refer to as scam schools. We meet with people at senior citizens' centers, health care

providers. Various organizations such as the University of Missouri Extension Service set up meetings for us, and we pass out information about these scams, and other things, as well.

We get the feedback from our clients that those meetings—and although we do not have a whole lot of cases based on this one scam, you know, where we are actually representing clients, if you go to a meeting and say, how many of you have had this scam where these people have called you wanting to do computer repair, about half the room raises their hand. Most of them know not to talk to them, luckily, but it is happening and it is happening more and more often, apparently. My mother-in-law, for one, gets one of these calls once a week from the same guy and has for six months, so it is just going on.

Once these scammers have got their hooks into these people, basically, what we tell them to do is, of course, change their passwords, change their bank accounts, and get a credit report, and that is how many of these people get to us, is they have got their credit report and seen something strange on it. They have gone to get a bank loan and they cannot get it because of something on their credit report, which is a whole another can of worms, which pushes these people from a legitimate bank over to a payday lender to get the money they need, which creates even more problems for them.

It takes time to correct credit reports. We have to help them get the reports together from the police or FTC complaints, whatever they have done, get them properly filed with the credit reporting agencies, get scam alerts put on their credit reports so that, at least for 90 days, no new accounts will get established by the scammers. By the time the people get to us, they have usually tried to do this on their own, and unsuccessfully. They do not have the wherewithal to get all these reports together and get them filed properly, so once the scam has taken place, there is really not a lot we can do. We do not have anybody we can sue. We cannot sue the scammers. They are not there.

We do end up defending a lot of credit card cases, where the scammers have gotten a credit card for one of these people and end up selling it to a debt buyer. The account goes to a debt buyer, who then goes after our client and sues them and we have to defend the case. Usually, we can get an affidavit of fraud and file it and the debt buyers will go away, but it is a problem that takes attorneys' time and it takes clients' money. If they cannot afford an attorney and they are not eligible for our services, then they end up having to pay somebody to do this.

It is a large problem for the low-income community and it has some—as Mr. Schiller said, you get to the point where you do not want to answer your phone. Computers for the low-income population, especially, are family affairs. I mean, you have got your kids who are going to school are using them. The older people are ordering things or getting on Facebook, whatever. There are all kinds of people in that household using that same computer, and if the scammer gets the right person—that is the reason they keep calling back over and over again. They are wanting to get somebody else to answer the phone to try this scam on.

In my mother-in-law's case, she is afraid her husband is going to answer the phone. He has got Parkinson's now and is going downhill a little bit, and she does not want him answering the phone because of this, so anyway, it is a large problem, and again, education seems to be the biggest clue, or the biggest thing we can do at this point, is get the word out about it so people do not talk to the scammers.

Thank you.

The CHAIRMAN. Thank you very much for your testimony.

Education is clearly a key part of solving this problem and one of the reasons why we are holding this series of hearings and hearing from people who have fallen victim, like Mr. Schiller, but I want to go back to a point that Mr. Finn made, that we really need, I believe he said, aggressive and unrelenting enforcement actions if we are really going to stop these scammers.

Mr. Schiller did everything right once he found out that he had been scammed. He went to local law enforcement. He went to the State attorney general's office. He filed a complaint with the FTC, and yet, as he said in his testimony, the chances of him ever recovering the $1,400 that he was scammed of—which is a lot of money—are very slim.

Ms. Greisman, I want to go to you in this regard. I know the FTC is taking—trying to go after these scammers. I understand how important it is for consumers to complain, file a complaint so that you can analyze and see patterns, but how many actual recoveries have you made that have resulted in restitution to the Mr. Schillers who are out there?

Ms. GREISMAN. Unfortunately, we do not have a great track record, I have to be candid about that, not for lack of trying. When we file these actions, we often file them as an ex parte TRO, and one of the first things we do if the court so authorizes it is freeze any assets in the United States. What we have seen with a number of cases that we filed, we believe a good chunk of the money is offshore. We have successfully obtained relief where there are U.S.-based assets, but if they are offshore, it is a huge challenge.

The CHAIRMAN. We know from this hearing and from others that we have had that, frequently, the scammers are offshore, too. We looked at the Jamaica lottery case where the answer became more cooperation with the local government and extraditing the criminals and putting them in jail, prosecuting them. What efforts are underway with India, in particular, since that seems to be a source of boiler rooms that engage in these frauds.

Ms. GREISMAN. Well, I would like to be cautiously optimistic we are making progress. As Mr. Finn mentioned in the testimony, we have had a number of meetings with them. We do think they have economic incentives to take this seriously and be as concerned about it as we are, and we are just going to have to see how our cooperation progresses.

The CHAIRMAN. Mr. Schiller, you mentioned to me that you worked for an Area Agency on Aging, that you actually put on telemarketing seminars to warn people against scams. You are obviously a very intelligent and knowledgeable individual, and yet Brad was able to convince you to give him access to your computer. Do you think that it was because it was a technology issue that you

were able to be convinced as opposed to if someone had called you up and said, you have won the lottery, just send us money and we will give you the payment? Do you think it was technology?

Mr. SCHILLER. I think you are right. Yes. You know, as I said, I know what an IPA is. It is your computer's identification number. How he had that out of that machine, I have no idea, plus my name, plus my phone number, with no prior indication at all that I had been hacked or anyhow invaded on that. I mean, it had not happened, so yes, he was coming from somewhere and that impressed me, and I do not know how I am going to even ever overcome that. I cannot understand—I am still scratching my head about Windows 10 now. You know, there is always a new world, the older you get.

Yes, it is a technological issue, but the principle is the same. If it sounds good, do not believe it.

The CHAIRMAN. I think that is good advice, and believe me, a lot of us, when we see upgrades, we always hesitate whether that is for real or is it someone trying to implant a virus into your system, so I am very sympathetic.

Finally, I just wanted you to share with everyone what happened just last week when the Committee staff was calling you to talk about this hearing. Who called?

Mr. SCHILLER. Someone from John—someone calling themselves, this is John Boehner. I am calling from the Microsoft Support Team. Microsoft has been getting reams and reams of error reports for weeks from your machine. Apparently, you are not paying attention to this.

The CHAIRMAN. Even in the midst of your preparation for this hearing, you got yet another call.

Mr. SCHILLER. That was Friday, yes.

The CHAIRMAN. Thank you.

Senator McCaskill.

Senator MCCASKILL. Thank you. I hate to be like a broken record. I know you know what is coming, Ms. Greisman, because we have been down this road before, and I know this is not your call, but we have got to put somebody in jail. We have got to put somebody in jail for these folks to take us seriously.

I would ask both you and Mr. Finn, with the diagnostics you have, Mr. Finn, and the capabilities you have, what do you see as the major impediment to imprisoning these people? I mean, if you look at the amount of money and time we spend going after robbers in this country, compare and contrast the amount of time and energy we spend going after robbers that are depriving seniors of their money, their dignity, and more importantly, isolating them.

What they are doing is beyond cruel, because if you are a senior and you feel like you cannot answer your phone, then your life can become incredibly lonely. Your life can be so limited to the walls in your home, your inability to be mobile, your inability to interact like you used to when you were much younger in social situations. It just is so frustrating to me that we cannot collectively get the political will to decide that some of these people need to go to prison.

Can either of you help me help you light a fire under local prosecutors or DOJ, because, you know, I know they are hard to catch,

but with your help, Mr. Finn, if your company and others like your company are serious, we can get them. We can get them much more effectively than if we try to do it without you.

Mr. FINN. We can. I think we can, Senator. I think, as Senator Collins said, these are ruthless criminals, and that means that they need to be dealt with in a very severe way.

I think one of the opportunities here is to leverage some of the capabilities that the Microsoft Digital Crimes Unit has to offer to law enforcement, and that includes using big data and analytics and visualization. These are—we have some technologies that enable us to better track and trace the cyber criminals, put the pieces of the puzzle together, and then actually quantify the harm.

Part of what I think is going on in the cybercrime space is that it feels invisible to a lot of people. It does not feel invisible to Mr. Schiller or to any of the millions of people who have been victimized by these phone calls, but I think, for some of the people sitting in difficult positions where they have to prioritize cases and they are looking for the evidence, it is not as easy or it is not as simple as maybe some other conventional crimes that law enforcement has worked on for years and years.

In the 21st century, where we have capabilities to use big data and analytics, the kinds of things that we at Microsoft have an opportunity to share, I think we can do things to fight cybercrime that can really make a difference and we are working very closely with the FTC, we are working closely with the State AGs, and I am pleased to say we are also now working closely with the FBI. We are sharing some of this big data and analytics. I think we can do much more to quantify the harm and then put these cases at the top of the priority list where they belong.

Senator MCCASKILL. Ms. Greisman, is there an effort, and maybe either one of you can speak to this, and perhaps even Mr. Polivick can speak to it, are we reporting under the Uniform Crime Statistics, the FBI, reporting crime statistics about these crimes? Are they—when communities are compiling how safe their communities are, are we even counting these crimes?

Ms. GREISMAN. I honestly do not know the answer to that. I can look into it.

Senator MCCASKILL. Do you know, Mr. Finn?

Mr. FINN. What I can say is I know that there are complaints made to the State AGs' offices. There are written complaints made to Microsoft. There are complaints made to the Senate. I think part of what is powerful about using the analytic tools is we can see the thousands and thousands of people who have clicked on the advertisements of the top criminal targets, so that is how you quantify it, because the fact is many of the victims are too ashamed, too embarrassed to come forward. Many of them do not come forward because they do not even know they have been a victim. They paid good money to solve a nonexistent problem, so they did not know it was a nonexistent problem.

Senator MCCASKILL. Right.

Mr. FINN. Our opportunity actually is to give a real clear, concrete shape to the problem which is otherwise invisible without the data.

Senator MCCASKILL. I know that Channel–3 has huge reach in Southwest Missouri. Have you had any luck with any of the—have you all reached out to any of the radio networks? I am thinking of some of our—as you well know, having—if you drive through the Delta area of the Bootheel, radio, local radio is still a very big presence in many Missourians' lives, especially in rural communities. Has there been any effort to reach out to MissouriNet or any of the networks to maybe feature scams on any of their programming?

Mr. POLIVICK. They are doing that to a certain extent, but I think it is the University of Missouri Extension Service that is doing that.

The CHAIRMAN. Would you turn your microphone on, please.

Mr. POLIVICK. I am sorry. Yes. The University of Missouri Extension Service is doing that to a certain extent in Southeast Missouri, as well as the television station in Cape Girardeau which serves most of the Bootheel——

Senator MCCASKILL. Right.

Mr. POLIVICK [continuing]. and Northern Arkansas. They do scam alerts quite often, not quite a weekly basis——

Senator MCCASKILL. Right.

Mr. POLIVICK [continuing]. but two or three times—two times a month, probably.

Senator MCCASKILL. Right.

Mr. POLIVICK. Yes, there are people doing that.

Senator MCCASKILL. Great. Thank you.

The CHAIRMAN. Senator Tillis.

Senator TILLIS. Thank you, Madam Chairman, for another very important meeting.

Mr. Schiller, you said you were the dummy on the panel, and I do not think you are a dummy at all. I think you are a very courageous person and I appreciate you being here and being willing to testify.

I had a quick question for you. When you said that this lowlife called Brad gave you a number, did you go onto a web browser and enter that number in? What exactly did you do with that number that he gave you over the phone?

Mr. SCHILLER. No. He read me the number, you know, like AB36N, whatever, to write down. I wrote it down. Then, with him on the phone, he walked me through some steps with my computer. The computer then generated that number.

Senator TILLIS. Got you. That kind of explains how he ended up getting into your PC. I was just kind of curious. One thing I will tell you, during this——

Mr. SCHILLER. Well, was that a chicken or the egg? I mean, if he had that number, did he get it out of my computer? I mean, he gave me the number, and then he——

Senator TILLIS. Yes. I think what you ultimately did was provide him—it is a common practice, Microsoft support and other legitimate technical support organizations, common practice for them to set up what they call an IP connection, a remote connection to potentially get into your computer, which is what enabled him to make your screen look funny and do the things that it did.

I will tell you, it is just about education. The reality is, somebody as educated and as informed as you, we will never get the broader

population probably as educated as you were with these scam artists working the way they are, which is why I want to get to enforcement and prosecution, but I will tell you, just a part of the education must be how much of your information is available online to make them seem like they are informed. In the time that the panelists were discussing, I went online. Either you or a family member had a CompuServe e-mail address at some point in time, and a lot of other indicative data. I could be Brad on the phone with something I did on my cell phone here.

Just a quick query. We need to let everybody know that if somebody calls you over the phone and pretends—under no circumstances would any legitimate technical organization approach you that way. It is the same thing with all the other scams that we have seen here, and I appreciate you being here to testify.

Ms. Greisman, this may not be for you—and Mr. Finn, I have a question for you about the underlying technology that Microsoft and some of the other major platform providers may be able to do to innovate and make this less likely to occur—but, has there been any thought given to trying to define the—you know, this guy Brad, I just want to call him a lowlife because we know that it is not his real name. There is kind of a criminal enterprise going on here. He happens to be the person on the phone, but in Mr. Schiller's testimony, you mentioned you called back, somebody else is on the phone. Has there been any thought given to trying to define this as a broader criminal enterprise, and would there be any advantage to doing that in terms of additional options for prosecution? Has there been any discussion along those lines?

Ms. GREISMAN. Not directly in that regard, but to follow-up on the criminal side, we do have a Criminal Liaison Unit whose sole goal is to get follow-on criminal prosecution on some of the consumer protection cases we have brought, because we know that what is going on is absolutely criminal. I assure you that that unit is extremely active and particularly active in this area.

Senator TILLIS. What about other leverage over—just because of the concentration of technology in India, it is not surprising to me that is one of the source countries. I am sure there are other ones. What sorts of discussions have we had with foreign jurisdictions to not only seek their cooperation, but potentially have a consequence if there seem to be these clusters within countries where they seem to be the biggest source of problems for the fraud occurring in the United States? What have we done there, or what kind of leverage do we have over other jurisdictions?

Ms. GREISMAN. Well, we have engaged in a number of meetings with India, in particular, and with other countries where we do see call centers targeting not just U.S. consumers, but English-speaking consumers throughout the country. A number of meetings have been had. We are working directly with not just law enforcement counterparts there—and law enforcement counterparts, I am referring both on the civil and criminal side—but industry. The legitimate call center industry in these countries has strong economic incentives not to lose American business, so I think that is another leverage point that we have.

Mr. FINN. If I could just—I just want to underscore a couple of things. First, Senator Tillis, I want to stress something you said

and I want to be clear on the education front. Microsoft will never make an unsolicited, cold telephone call to someone about technical support.

Senator TILLIS. Is that also true of your certified partners?

Mr. FINN. It is a little bit harder for me to say what everybody else will do, but you will never get a call from Microsoft in that way.

Senator TILLIS. It could be a good consideration for your certification program, to make them adhere to the same.

Mr. FINN. They cannot. Our certified partners, that is not the practice, but if there are partners who are doing this, they should be prosecuted, as well, I will say.

Senator TILLIS. Go ahead.

Mr. FINN. The only other thing I wanted to add to your question about the criminal laws, I mean, when I was a prosecutor at the U.S. Attorney's Office in New York City, I mean, the bank fraud statutes that we have used for years and years, those would apply to this conduct. The wire fraud statutes would apply to this conduct, and as you pointed out in terms of the kind of enterprises behind this, even the RICO statute might apply to this statute, so there are old tools in the prosecutors' tool chest that would apply, and there would be some new ones, the Computer Fraud and Abuse Act, as well, but the fact is, there are some bedrock criminal statutes that can be used to really hold these people accountable.

Senator TILLIS. Well, one final question, Chair, if I may. The technology providers, in particular, I think, are at a position where at least if—if I think the manner that was used to get access to Mr. Schiller's computer—what sort of work is Microsoft doing? I know you are not in the R&D department, but what sort of work are you all doing to provide a warning—because basically what you are doing is opening up the back door to your computer, which is what allows some of these—not all the scams, because some of them are just pure acting out on the phone, but what sorts of additional layers of protection are you providing? That is one question.

The other one, right now, with Windows 10 upgrade being pervasive, a lot of people going through it, some of them going through technical problems, my guess is a year from now we are going to see an uptick in some of these scams because they are ripe for it. There can be apparently legitimate reasons why you need tech support while you are going through the upgrade. Mine went fine, by the way, and mine is a relatively new computer, but I think that we have to even have a heightened concern, because there are tens of millions of Microsoft-based platforms that are going to go through an upgrade over the next 12 to 14 months. What steps are you all taking to make sure that they do not take advantage of this transition?

Mr. FINN. Well, one of the most significant features in Windows 10 are some security capabilities, including that Windows Defender is built into Windows–10, so that is a capability that is going to help protect computer users in a new way and a significant way, so that is the first thing I would say.

I think the second thing is, we have seen some of these scammers. I mean, it is all about winning over the trust of the victim, so they are going to leverage the names of reputable brands,

like Microsoft, to win the trust, and then one of the things they do that is particularly cunning is they do things like what Mr. Schiller pointed out, ask Mr. Schiller to run certain commands and then the screen looks to a non-technical person like something is a miss, and one of those things is a vent viewer, and that can show apparent error messages. Those error messages are very benign, but they are actually very useful for IT pros when it comes to troubleshooting, so they are useful.

I will say that the people at the company are aware of what criminals are doing and we are constantly trying to simplify these things, but we recognize that the criminals will be shrewd and cunning and we need to react, as well.

The CHAIRMAN. Thank you.

Senator Kaine.

Senator KAINE. Thank you, Madam Chairwoman, and thank you to the witnesses for the testimony.

Mr. Finn, you mentioned in your testimony briefly that Microsoft has a partnership with AARP that is focusing upon some consumer education and I wondered if you might elaborate on that a little bit more. Talk to us about that partnership.

Mr. FINN. Sure, Senator. We recognize that education is so important, we are doing things with AARP. We have started to have these scam jams where we bring people from the AARP—se have senior Microsoft leaders there, too—to talk through the issues, some of them—in the same way this hearing is shining a light on the problem, we want to shine a light on it and then give the tips, the tips like a Microsoft—Microsoft will never make an unsolicited call to you. Tips like, do not click on a pop-up that says your machine is infected. You know, if you have a problem, contact support.microsoft.com. Contact Microsoft's customer assistance if you have a problem. Contact the customer assistance line of the computing manufacturer. We want to make sure that seniors and others really can avoid this sort of victimization that we hear so much about, and we are doing these trainings in some of our retail stores around the country, so there is a lot we know we have to do. I really agree with the fellow witnesses that education is important and we need to keep working on that.

Senator KAINE. Thank you.

Ms. Greisman, you were talking about the call centers and maybe targeting some of the call centers, in particular, you were talking about in India, but wherever they are. Are some of these scams coming out of call centers that are not just illegitimate, but do plenty of legitimate business, too, and then this is just kind of like a little component of what is going on in the call center?

Ms. GREISMAN. That is a good point. We do have a real concern that in India and perhaps in other countries, there are small pockets of operations in an otherwise larger call center that is otherwise legitimate, whether they just have too much extra capacity, too much extra bandwidth and are using it for illegal purposes, but that is a real suspicion that we have.

Senator KAINE. You know, if that suspicion could reach an appropriate level, you know, putting lists of call centers on, you know, as you are doing commercial work and you want to do work with call centers, and so many companies do, here are some call centers

that are under the subject of some active investigation right now, it might warn American companies away from using certain call centers. We should make it painful on anybody who is trying to do legitimate business, make them self-enforced and make sure that there is not illegitimate business being conducted in that location, so that is just a thought, and I will tell you, the last thing I want to say is this to the Chair and Ranking Member. I am relatively new to this Committee. You know, this Committee is making me a very suspicious person.

I was not so suspicious when I got here, and I will just tell you, I was just thinking of one today, I mean, literally as we are having this hearing. Somebody came up to me the other day and said, "I send you e-mails all the time and you never respond." Now, that is just not the way my office operates, but I took his name and information and I went back and I said, here is this senior citizen who says he sends us e-mails and we do not respond. Well, we were able to track three instances. He had sent us an e-mail and we had responded. We reached back out to him. He acknowledged those, but, he said, "No, but I have sent you so many since then and you never respond." It looks like what is happening is he is not sending e-mails to us but some advocacy organization is maybe reaching out to him——

Senator DONNELLY. They are actually going to my office——

Senator KAINE [continuing]. and asking him to do e-mails, but it may be that the advocacy organizations—I mean, it did not occur to me. We were just talking. We are trying to figure out, okay, good. We are responding to his e-mails. That is great, so now we do not have a problem. Now I am sitting here thinking, well, maybe this, "advocacy organization" does not have anything to do with advocacy and maybe they are just trying to get him, and maybe get some information from him and say they are going to forward the e-mail to the Senate, but the whole thing may be some information fishing operation, and I did not think of it until during the middle of Mr. Schiller's testimony.

I have got more work for my staff to do when I go back to the office, so thank you for making me a suspicious person.

The CHAIRMAN. Thank you, Senator.

Senator Donnelly.

Senator DONNELLY. Thank you, Madam Chair.

Mr. Finn, Indiana's Attorney General's Office has reported 48 complaints this past year related to tech support scams and 13 consumers falling victim to that. Microsoft—in your testimony, you said it believes that this is one of the largest forms of fraud against consumers in the United States. Can you describe the scale of this problem from Microsoft's perspective?

Mr. FINN. Sure, Senator. I think our indications are that the quantity of people who have been harmed is really—way exceeds the sort of numbers of just the people who complain. The facts are that many people who have been victimized are too embarrassed, too ashamed to come forward, so complaint statistics alone are not the best indicator. In addition, a lot of the people who have been victimized do not even know they have been victims because they purchased something that they thought was solving a problem, and, of course, it was not a problem at all, but we also have data

that tells us that it is much, much larger. We believe that the number of people who are harmed is 3.3 million people annually at a cost of $1.5 billion, so that is the full statistics.

I can tell you, Senator, that just in the State of Indiana—I mentioned before that we can use big data and analytics to see some things that you cannot just see through anecdotal and individual complaint reports. In the State of Indiana just in the last 90 days, from the top six companies that we believe are criminal organizations stealing from people, including many senior citizens around the country, there have been 245,000 times—individual times—that advertisements from these criminal organizations appeared to Indiana—on the machines of Indiana residents.

Senator DONNELLY. This is in a State with 6.6 million people.

Mr. FINN. Right, and that is just ninety days, and that is just on our search engine. The facts are that the complaints are significant and we can use that, use that in criminal cases, but the opportunity here, as I have said before, is that if we harness the big data and analytic capability that Microsoft's Digital Crimes Unit feels we must and that we are sharing with law enforcement, we really have an opportunity, I think, to do so much more in this space to protect people.

Senator DONNELLY. Well, let me ask you about this. Another woman from Indiana got a cold call and it said there was a problem with your computer. She did not have a computer, so she was able to deal with that, but for those who do, when that call comes in, what are some of the things you can do to detect that call, to deal with it, to handle it? What are some of the best recommendations that you have?

Mr. FINN. Well, the first thing is, you get a call from someone that is unsolicited talking about technical support, hang up. That is the first thing. That is not a legitimate effort to sell anything to you, so that is the most important message, I think, to people if they get that phone call. Do not continue it. Hang up.

We do know that people do sometimes have malicious software on their machines and they may need help, and for that reason, we really suggest to them they contact Microsoft. They contact our customer support. They contact the manufacturer of the computing device, contact their customer support, and the fact is, there are hundreds, thousands of reputable companies who provide technical support to people. The guidance is simply, just as if you have a problem with your car and you want to go find a mechanic, you are careful about what mechanic you go to. You want to have someone you trust and you have heard is a good mechanic, an honest one. I would say that the same thing goes for finding help with your technical help.

Senator DONNELLY. Well, let me ask you this. Back about a year ago, in August 2014, I held a field hearing back in Indiana on scams against seniors, and we have a great group in our State, and I know other states do, too, the Senior Medicare Patrol Program, to try to help seniors to avoid these kind of things.

This would be to the whole panel. What is your best recommendation, what you have found to be the most productive, most helpful, in trying to warn seniors of what might be coming

down the line in terms of scams against them, what to look out for, what to deal with.

Mr. Schiller, I want to thank you for being here, for spending this time to be with us today, because your telling us your situation that you found yourself in is going to help someone else to not have to deal with that, and that is what people from Maine do, is it not, Madam Chair?

The CHAIRMAN. Absolutely.

Senator DONNELLY. Yes. If anybody would like to tell us, hey, here is my best recommendation for our seniors as to how to avoid these kind of things, and if one starts on their phone or in their computer, what to do next. Ms. Greisman.

Ms. GREISMAN. Yes, thank you. What Mr. Finn said is absolutely right. Hang up. Hang up and file a complaint with whatever information you may have received.

The FTC has done a lot of research on how to best communicate with older consumers, and that is what "Pass It On" is really a product of, and what we found is that it is important to empower seniors to assist their friends and families and not to feel victimized or feel that they are, for some reason, vulnerable. On the contrary, to make them feel like they are in the best position to ward off a scam.

Senator DONNELLY. Okay. Thank you very much.

Thank you, Madam Chair.

The CHAIRMAN. Thank you very much.

Senator Blumenthal.

Senator BLUMENTHAL. Thank you, Madam Chair, and thanks for holding this hearing. Thank you all for being here today.

I know a little bit about elder justice from my days as Attorney General in the State of Connecticut and am very pleased to see the FTC ably represented here today. Thank you for all your good work.

I know from my own experience here in the Senate, as well, the importance of fighting these scams and raising awareness, as you have just said. I do not know how many times I have said, hang up, or if it looks too good to be true, it probably is. Why do you think—and I will pose this question to all of the members of the panel—why do you think that hope continues to spring eternal unrealistically and seniors continue to be bedeviled and confused and misled and deceived by these kinds of scams? Many of them seem obvious to us.

I proposed a bill, the Robert Matava bill with Senator Ayotte, that seeks to combat this kind of fraud, named after a World War II veteran, a Marine, who was himself horrifically abused by elder fraud, and yet disbelief seems so difficult to invoke. Why do you think it is?

Ms. GREISMAN. I wish I had a ready answer to that. Certainly, some people are simply more open to contact with total strangers than others. Some people will not do it at all. There is not enough—in my view, there is not enough research on the very issue that you raise so that we actually could be better informed, and it would probably help us target our educational materials in a better way. We have done a good deal of research in this area, but more on victimization is needed.

Senator BLUMENTHAL. It really is important to know, because if you are going to target solutions, if you are going to try to deal with human nature, perhaps the tools that the bad guys use ought to be used more artfully or ingeniously by the good guys to try to reach these very vulnerable seniors.

Ms. GREISMAN. The work that we have done with the AARP Foundation, I think, does address several of the points you raise, because that is one-on-one peer counseling and there is data to suggest that that type of counseling makes it less likely a person will be revictimized.

Senator BLUMENTHAL. Mr. Finn, as a service provider, you obviously bring to the table an important perspective as we examine these kinds of fraud, and I was alarmed to learn that some companies are, in fact, profiting from scam artists purchasing fraudulent ads. In one instance, the FTC found that since 2010, a network of scammers have paid Google more than a million dollars for ads and for certain key terms.

I was pleased to see that Microsoft has been proactive in removing and screening fraudulent tech support ads from your Bing search platform, which I think is commendable, and I wonder if you could explain why this issue persists in similar platforms and what best practices you would recommend for other providers.

Mr. FINN. Well, I can comment on we do at Microsoft, and we do take affirmative steps to not allow criminals to use our platform to harm people, and so, one of the ways we do that is we invest in automated systems to monitor some of those organizations. We invest in manual methods of seeing who are the organizations advertising on Bing, and when we see that they are doing things that are harmful, that are taking money from people illegally, we kick them off, so that is one piece that we do, Senator.

I think the other thing we do is, obviously, we have invested in a lot of the education efforts with the AARP and education that we do in our retail stores around the country. I think the fact that we have a team like the Digital Crimes Unit is a testament to how important we think it is as an industry leader to protect people and make sure that technology is something people can trust.

I think there are a number of things that we feel it is important to do, and we know we have a lot more to do. We have certainly reinvigorated the work in this space because the complaints have increased by 60 percent in just the last eight months. This is not a problem that is going away. It is getting bigger. That is why we really need to do even more, and again, why I am so appreciative of this Committee and Chairman Collins for shining a light on the problem, because I think we all agree more needs to be done to protect our seniors and other people using computing devices in the country.

Senator BLUMENTHAL. Thank you. Thank you all, and I join your thanks to Senator Collins for having this hearing. Thank you.

The CHAIRMAN. Thank you.

I am going to ask one final question of Mr. Finn and then give my colleagues an opportunity for a final question, as well. You have some fascinating data in the appendix to your written testimony, and I would like to focus on one of the charts. It is a little difficult to understand when you first look at it, but it is really illu-

minating in terms of how big a problem this is. Could you walk us through what it is we are looking at just so everyone can understand how serious this problem is.

Mr. FINN. Sure, and Chairman Collins, I just think it is—this is a great opportunity, I hope, to illustrate the power of data and analytics and visualization, because what you are looking at is a map of the United States and you see lots of colors, first of all, there. The resolution, you cannot really distinguish too many, but there are six different colors, and those colors represent the six top targets of our investigations that we are working on with the State AGs and with the FBI. They represent individual instances across the United States where a user of a computing device clicked on one of the ads of one of these six companies engaged in criminal activity.

The taller the tower, so the higher the bar, indicates a large volume in a particular location, but what you are really seeing, 462,000 times over just a 90-day period, American citizens clicked on the links of companies engaged in really horrific, as you said, Chairman Collins, ruthless activity designed to steal from people.

The power of—and as a former prosecutor, those are 462,000 attempted criminal acts, and it is probably the case that many, many, many of these were converted into illegal gains that the criminals took, where they basically took that money from citizens of the country, and that is just 90 days on just Bing.

The CHAIRMAN. I am so glad that you gave us this chart, because it really illustrates how explosive and widespread this problem is. As you said, and I want to reemphasize it, you found 462,000 clicks, and this is just in 90 days and just targeting six companies. That is extraordinary, and you are one company, one effort—granted, a large company, but to me, this just cries out for a more aggressive approach by law enforcement. I thought Senator McCaskill put it very well when she said that if you had that pattern in robberies, law enforcement would be all over it. Well, this is robbery, as well, using technology, and it seems to me it deserves far more attention.

I also wanted to point out your educational brochure that you have done with AARP on how to avoid tech support scams. It goes along with the FTC's efforts, and I think we need more of the education, as well.

Let me just end my questions and comments with a personal story that will show you that education alone cannot take care of the problem. Last week, I received an e-mail from, it appeared, my credit card company telling me that suspicious activity had been detected and asking me to call a 1–800 number. Well, I am suspicious enough that I thought the e-mail was fraudulent. It was not a 1–800 number. It was a regular number. I called the number. They immediately asked me for my Social Security number. Well, that was a big red flag, so I said no and hung up. Well, guess what, it was legitimate.

It is extremely difficult to tell whether or not you are dealing with a fraudulent situation, which this had all the hallmarks of, an unsolicited e-mail, a number to call, and a request for my Social Security number. That would be in your brochures telling me to

hang up. Yet, it turned out, even though I had my credit card with me, that, somehow, someone had gotten my credit card number.

What I did was call the number on the back of the card rather than the number that was in the e-mail, but Mr. Schiller, believe me, I will second what Senator Tillis said. You are no dummy at all. You are a very intelligent individual, and this can happen to any of us, even those of us who are very wary of this situation, and that is why I think in the end, the answer is more law enforcement actions, because that will not only punish the criminals—and let us remember, that is what they are, they are criminals—but it also will deter others from perpetrating these frauds.

I very much appreciate all of the testimony today. I want to give Senator McCaskill and Senator Tillis the opportunity for another question or any comments that you want to make before I close the hearing.

Senator MCCASKILL. I just appreciate everyone being here. I certainly appreciate you, Mr. Schiller. There is nothing that is harder than saying publicly, I have been had. You doing this is a great service to your country and to other people who are potential victims down the line, and we are all very proud of you for doing it.

Thank you to Mr. Polivick for traveling here from Missouri. I think I wish in some ways we could have someone from legal services that would sit on this dais with us in lots of hearings, because what you see every day is what we need to be fighting for, and that is people who are working hard, playing by the rules, having a hard time keeping their head above water, and the last thing you need is some con artist, bottom feeder scum trying to feed off their lives when they are having a hard enough time keeping their head up, so I hope that legal services is maintaining its fundraising. I know the government funding has waned and waxed and mostly waned——

Mr. POLIVICK. Mostly waned.

Senator MCCASKILL. Mostly waned, especially in my State.

Mr. POLIVICK. Well, like our clients, the legal aid programs are constantly playing catch up, you know, trying to get enough funding to keep up with what needs to be done. Our clients are not able to get caught up when they are dealing with scams like this. It is just another blow that they cannot stand.

Senator MCCASKILL. Thank you. Thank you, all of you, for being here.

The CHAIRMAN. Thank you.

Senator Tillis.

Senator TILLIS. Thank you, Madam Chair.

Just a quick question. Ms. Greisman, Mr. Finn's comments about the kind of self-policing they are doing at least with these six Internet presences raises a question. You get them all the time if you are on the Internet. Your PC may be infected, click this button, and it could actually either open a door or get you to buy something you do not really need. At what point—I mean, are the laws or the rules that we have on the books now sufficient for us to go to a—we are just talking about Bing searches. If you overlaid this diagram over the same period of time with the Google engine, Yahoo!, and a number of other search engines out there, the multiplier would be astounding.

What could we do to make it an illegal act to even request the kinds of ads that Microsoft have identified and taken down? What more can we do on a proactive basis to reduce the flow of actions that a Microsoft or a private sector company would even have to deal with?

Ms. GREISMAN. I am not sure there is a simple answer to that question. Certainly, ad screening. Microsoft is doing it. We talked to a lot of other search engines out there and a lot of other advertisers, network advertisers, about improving and enhancing their ad screening techniques. I am not sure what more could be done at that level.

Senator TILLIS. The only other thing I will mention, you know, when we have this discussion, we all think about the desktop PC or the laptop, but the same problem occurs here or the same pop-ups occur here. There are hundreds of millions of devices that these—I like "scum" better than "lowlife," by the way, Senator McCaskill——

[Laughter.] [continuing.] that they are using to prey on innocent, trusting people, but we need to make sure that the FTC, the other government agencies are being innovative in additional things that we may need to take action on to provide you with more tools, and we certainly, because of the wealth of expertise that a Microsoft and some of the top tier platform providers have to offer, you need to be coming with us to tell us what more we can do to enable you to provide products and services that get after these people.

Thank you all for being here. Mr. Schiller, thank you.

Ms. GREISMAN. Thank you.

The CHAIRMAN. Thank you, Senator.

Committee members will have until Friday, October 30th, to submit any additional questions for the record.

I want to again thank all of our witnesses today, particularly my constituent, Mr. Schiller, who came from Peaks Island to share his experience, but all of our witnesses were extremely helpful.

I also want to thank Senator Tillis and, of course, my Ranking Member, Senator McCaskill, and all of the other members who participated in today's hearing, and I want to thank our staff, which has done a great deal of work to put together a whole series of hearings on what appear to be an endless number of scams that are targeting our seniors.

We are going to continue our investigations, and I want to second Senator Tillis' comment that if legislative changes are needed to increase authority to go after these scammers or create new laws that enable them to be prosecuted, we would welcome your suggestions and would work closely with you. Thank you very much for your testimony.

This concludes the hearing.

[Whereupon, at 3:57 p.m., the Committee was adjourned.]

APPENDIX

Prepared Witness Statements

Testimony before the United States Senate Special Committee on Aging

"Virtual Victims: When Computer Tech Support Becomes a Scam"

Testimony of Frank Schiller

October 21, 2015, 2:30 p.m.

562 Dirksen Senate Office Building, Washington, D.C.

Good afternoon, Chairman Collins, Ranking Member McCaskill, and distinguished members of the Committee. I am Frank Schiller from Peaks Island, Maine, and I appreciate the opportunity to be here today to share my story as a victim of a computer scam. While the whole episode was extremely embarrassing, I wanted to share my story with you today out of my concern that these criminals are still preying upon seniors and others. They need to be stopped and their calls rejected.

On October 1, 2013, I received a call at home from someone calling himself Brad. Brad, perhaps not his real name, said he worked for Kavish Techno Software, a company under contract with Microsoft. He claimed they had identified many problems with my computer's operations. He gave me a 32 character alpha-numeric, asked me to write it down, and said he could verify the problems for me if I got on the computer, which I did. After I typed a few of Brad's keyboard instructions, my screen displayed the same 32 character alpha-numeric he had me write down. He said that this was my computer's ID and I should not show that number to anyone. After several more instructed keyboard entries, my screen showed a huge number of small files (that had no relation to anything I knew of) that he said were indicative of problems clogging up my computer. How had he known my name, phone number, and computer IP Address? I don't know. But this technological savvy allayed my concerns about the legitimacy of his business.

He said they had software to clean the computer and to stop the malicious files. He presented several options varying in price. I eventually agreed to the larger, longer term package of $349 for one and $79 for another program. I gave him my Visa number to pay for the two software programs. He then said that Visa would not authorize payment because his company had to use the Central Bank of India, overseas, so I would have to authorize Visa directly. He gave me a phone number with a 190 area code to call him back. When I did, someone else answered (no company greeting) and transferred me to Brad. My Visa was charged a total of $428 for the two software programs. I then ran one of the two software programs, but it didn't seem to affect my computer positively or negatively and my computer seemed to be operating as it was before this incident. I later discovered that a folder labeled "Support" had been installed on my desktop. In this folder were two receipts for the two charges to my Visa card from the Central Bank of India. The third file was a "Contact Me" memo with the company name, phone number, and e-mail addresses. I have not attempted to contact the phone number or the e-mail addresses.

On December 16, 2013, I received another call from Brad. He said that his company's contract with Microsoft had been canceled and therefore he would need to refund the money I

had paid for the two software programs. I asked that he send me a check, but he said the refund had to be completed using the same form of payment as the original transactions (Visa). However, he said that Visa would not accept the credit. He instructed me to go online and follow his keyboard instructions so he could transfer the refund to my checking account. Maybe I should have questioned this more, but given that it was shortly before Christmas and he was offering a refund for software that seemed fairly worthless anyway, I fell for it, following the keyboard instructions and typing my routing and account numbers into the screen that appeared which I recognized as Western Union. Quickly, the screen was miniaturized and flashing so it was difficult for me to see what was happening. I caught a glimpse of $980 being typed into one of the fields, but the whole process happened very quickly. I later determined that the keyboard instructions I followed allowed Brad to control my desktop. Once I entered the account and routing numbers, he was able to complete the rest of the transaction remotely.

The next day (December 17, 2013), I discovered that $980 had been withdrawn from my checking account. The day after that (December 18, 2013), I called the bank and froze the account. I then noticed that a program called Teamviewer had been installed on my computer. I uninstalled it. Brad called again that day and wanted to access my computer, but I refused.

The day after that (December 19, 2013), I called the Portland police department to report the crime. Randy Richardson, a patrol officer from the police department, visited my home and took my report. While he was very sympathetic, he assured me that since Brad and his cohorts were likely overseas, it was unlikely any of my money would ever be recovered. I did e-mail Western Union to alert them of this fraud.

The next day (December 20, 2013), I closed the checking account. Shortly after (December 23, 2013), I sent a formal complaint to Western Union about an additional $25 that had been withdrawn from my bank account to cover the service charge for the transaction. In total, I lost $1433 to these scammers.

In March 2014, I also contacted the Maine Attorney General, the Maine State Police Computer Crimes Unit, and the Federal Trade Commission (FTC) to report this crime out of concern for others who may be victimized by these criminals. I did receive a letter from the Maine Attorney General's office and the FTC gave me the number for a counselor and a complaint number for my case. To date, other scammers, seemingly from the same outfit and the same story about a Microsoft refund, continue to call me several times a week offering to fix my non-existent computer problems. Brad himself has never called back as far as I can tell. Usually they call in the morning and sometimes several times in the same day. I usually say I'm busy and ask for their phone numbers so I can call back later and also ask them where they are calling from. They have no answers to my questions, only demands. In fact, just last Friday, in between calls from the Majority Aging staff regarding today's hearing, David Bonner, supposedly from Microsoft Technical Support, called offering to update my computer. I hung up on him.

I realize that any chance of financial recovery is near zero. I came here today to share my story with you hoping that it may help other people from falling for these scams and also to assist the Committee, federal law enforcement, and companies like Microsoft in their work to put these criminals out of business. As someone who for many years worked with seniors on a daily basis

warning them to be vigilant to telemarketing schemes, I cannot believe I fell for one. If it could happen to me, it could happen to anyone so I implore you to do anything you can to put a stop to this and get the message out that if the scammers keep this up, they will be caught and suffer the consequences for defrauding seniors like me.

Chairman Collins, Ranking Member McCaskill, and members of the Committee: I appreciate your interest in my story and your leadership on this issue, and I will do my best to answer any questions you may have. Thank you.

Prepared Statement of Lois Greisman
The Federal Trade Commission

Before the
United States Senate
Special Committee on Aging

on

Combatting Technical Support Scams

Washington, DC
October 21, 2015

Chairman Collins, Ranking Member McCaskill, and members of the Subcommittee, I am Lois Greisman, Associate Director of the Division of Marketing Practices, Bureau of Consumer Protection at the Federal Trade Commission ("Commission" or "FTC").[1] I appreciate the opportunity to appear before you today to discuss the Commission's initiatives to fight illegal tech support scams.

"There is a problem with your computer. I will help you fix it." This is a typical opening line from a script scammers use to deceive consumers into purchasing unnecessary, worthless, or even harmful services. These tech support scams then charge hundreds of dollars to "fix" non-existent problems, leading consumers to believe that the tech support worked when, in fact, their computers never had a problem. Based on the FTC's consumer complaint data from January 1 through August 31, 2015, these nefarious scams appear to have a disproportionate impact on older consumers[2]: of the more than 18,000 tech support complainants to the FTC who reported their age,[3] 76% are over 50; 56% are over 60 years old.

The FTC is working hard to combat this problem. After explaining tech support scams in greater detail, this testimony describes the Commission's efforts to combat these scams on three fronts: (1) our aggressive law enforcement; (2) our work with international partners; and (3) our robust consumer and business outreach.

---

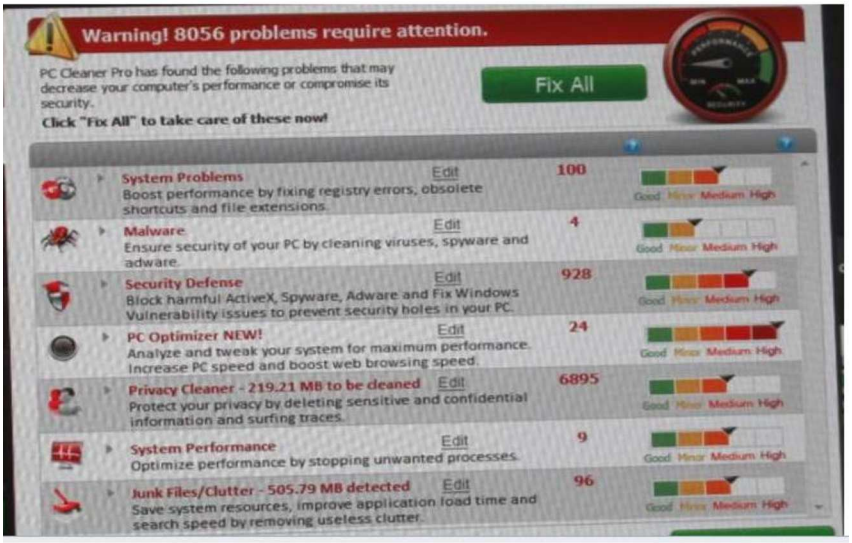
[1] The views expressed in this statement represent the views of the Commission. My oral presentation and responses to questions are my own and do not necessarily reflect the views of the Commission or any individual Commissioner.

[2] References in this testimony to "seniors" or "older" individuals means the population 65 years and over, unless noted otherwise.

[3] The FTC's Consumer Sentinel is a portal for consumers to report complaints. Providing personal information such as age is not required.

I. Tech Support Scams

Tech support scams use various methods to convince consumers they have a problem with their computers. Some scammers call consumers and falsely claim they are calling on behalf of a well-known company like Microsoft, Facebook, McAfee, or Symantec, and that they have detected a problem on consumers' computers. Others use deceptive computer pop-up messages that claim consumers' computers have a problem, or offer free system "scans" that mark innocuous computer files as "errors," and then direct consumers to call a specified phone number to fix the purported problem. The following screenshot shows the results of such a system scan, which claimed an uninfected FTC computer had "8056 problems requir[ing] attention":

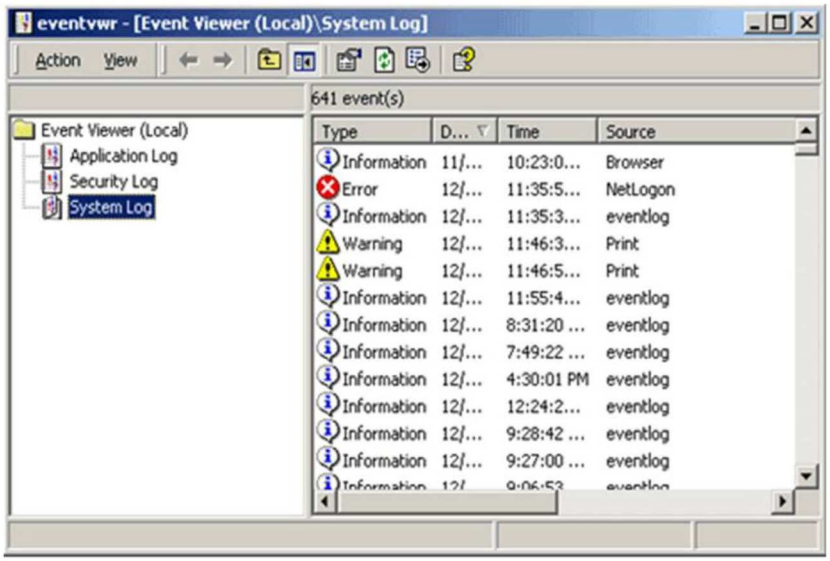


Still other scammers place advertisements with search engines that appear when consumers search for their computer company's tech support telephone number.

Once scammers have consumers on the phone, telemarketers try to convince consumers that their computers have been infected with malicious software or suffer from significant "errors." The scam artists further claim that unless these consumers agree to pay for "technical support" to fix the problem, their computers will crash, and they will lose all of their data. By convincing consumers that their computers have problems, scammers induce consumers to buy services and software they do not need.

These tech support scam artists go to great lengths to add authenticity and urgency to these calls. The telemarketer often connects to the consumer's computer through an online platform such as LogMeIn.com. Once connected, the telemarketer typically opens a utility program, such as "Event Viewer," on the consumer's computer and falsely claims that "errors" and "warnings" shown on Event Viewer demonstrate that the computer is infected or in need of repair, as shown in the following screenshot:

Sample Event Viewer Log



The telemarketer intentionally does not tell the consumer that the Event Viewer program usually displays a large number of warnings and errors even for a completely normal Windows computer system. Such warnings and errors are typically due to routine activities and may be present even if the machine is in perfect operating order, yet the scammer claims they are a sign of significant system damage. For example, a tech support scammer navigated an undercover FTC investigator's computer to a screen similar to the one pictured above and then made the following false claims to the investigator:

> You have downloaded these unwanted malicious programs without your knowledge, ma'am. Whenever you go online, whenever you browse the Internet,

> this [sic] errors and warnings that it's getting downloaded without your knowledge and it is destroying your computer day-by-day.[4]

After extensive conversation and repeated warnings to the consumer that she is at grave risk of losing all her data, the telemarketer eventually offers to repair the problem. In the undercover call mentioned above, the scammer charged $199 for unnecessary "repairs."

It is easy to understand how consumers, especially those with limited computer skills, would believe this tech support scam and purchase the scammers' "repair" services.

Consumer complaints filed with the FTC illustrate the scope of the tech support scam problem. In response to mounting evidence that tech support scams were victimizing American consumers, the FTC created a new complaint category in January 2015 called "tech support scams." As of August 2015, we received 23,709 complaints filed under the "tech support scams" category, with reported consumer loss of more than $5 million.[5] These figures, however, undoubtedly understate the problem. The FTC knows from law enforcement experience that many consumers never file complaints. Here, the lack of reporting is exacerbated by the fact that many consumers do not even realize they have been victimized. As our cases have shown, many consumers' computers may run smoothly after they pay for the scammers' unnecessary services (because there was likely nothing wrong with the computers in the first place), and consumers may not realize that they did not need the services they purchased.

---

[4] *FTC v. PCCare247 Inc.*, No. 12-civ-7189 (Docket Entry 11, Exh. 27).

[5] As noted above, more than 18,000 of these complainants provided age information.

II. Law Enforcement

The FTC has responded to the burgeoning problem of tech support scams with aggressive law enforcement.[6] In October 2012, the FTC launched a major international crackdown, halting six tech support scams primarily based in India that targeted consumers in the United States and other English-speaking countries.[7] The FTC coordinated this crackdown with the assistance of authorities in Australia, Canada, Ireland, New Zealand, and the United Kingdom.

The FTC obtained final judgments and orders against all of the defendants in these cases. Among other things, the orders prohibited all of the defendants from advertising, marketing, or selling any computer-related tech support services and from making misrepresentations. The Court also imposed more than $6 million in monetary judgments.[8]

---

[6] The FTC pursues deceptive tech support scams using its authority under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 and, where appropriate, the Telemarketing Sales Rule, 16 C.F.R. Part 310.

[7] *See* Press Release, FTC Halts Massive Tech Support Scams (October 3, 2012), *available at* www.ftc.gov/news-events/press-releases/2012/10/ftc-halts-massive-tech-support-scams; *see also FTC v. Pecon Software Ltd.,* No. 12-civ-7186 (S.D.N.Y. Sept. 25, 2012), *available at* www.ftc.gov/enforcement/cases-proceedings/1123118/pecon-software-ltd-et-al; *FTC v. PCCare247 Inc.,* No. 12-civ-7189, *available at* www.ftc.gov/enforcement/cases-proceedings/122-3243-x120057/pccare247-inc-et-al; *FTC v. Lakshmi Infosoul Services Pvt. Ltd,* No. 12-civ-7191, *available at* www.ftc.gov/enforcement/cases-proceedings/1223245/lakshmi-infosoul-services-pvt-ltd; *FTC v. Mikael Marczak, et al.*, No. 12-civ-7192, *available at* www.ftc.gov/enforcement/cases-proceedings/1223246/virtual-pc-solutions-mikael-marczak-aka-michael-marczak-et-al; *FTC v. Finmaestros LLC et al*., No. 12-civ-7195, *available at* www.ftc.gov/enforcement/cases-proceedings/1223247/finmaestros-llc-et-al.

[8] *See FTC v. Mikael Marczak, et al.*, No. 12-civ-7192, *available at* www.ftc.gov/sites/default/files/documents/cases/2013/05/130517marczakstip.pdf; *FTC v. PCCare247 Inc.,* No. 12-civ-7189, *available at* www.ftc.gov/sites/default/files/documents/cases/2013/05/130517pccarestip.pdf; *FTC v. PCCare247 Inc.,* No. 12-civ-7189, *available at* https://www.ftc.gov/news-events/press-releases/2013/11/tech-support-scheme-participant-settles-ftc-charges; *FTC v. Pecon Software Ltd.*, No. 12-civ-7186, *available at* www.ftc.gov/system/files/documents/cases/140724peconorder.pdf; *FTC v. Mikael Marczak, et al.*, No. 12-civ-7192, *available at* www.ftc.gov/system/files/documents/cases/140724marczakorder.pdf; *FTC v. Finmaestros LLC et al*., No. 12-civ-7195, *available at* www.ftc.gov/system/files/documents/cases/140724finmaestrosorder.pdf; *FTC v. Lakshmi Infosoul Services Pvt. Ltd.,* No. 12-civ-7191, *available at*

Last year, the FTC filed three additional cases against tech support scams. The FTC alleges that these scams have harmed thousands of consumers in the United States, resulting in more than $100 million dollars in injury.[9] Defendants in one of these cases, based in New York but again involving call centers in India, recently agreed to relinquish most of their assets. The owners are also prohibited from engaging in deceptive telemarketing practices and their websites have been shut down.[10]

The two most recently filed cases remain in litigation. In those cases, the FTC is seeking injunctive relief to stop the alleged deceptive practices and provide redress for consumers.[11] In each of those cases, the call center is in Florida. The agency continues to actively seek law enforcement targets and has additional investigations underway.

---

www.ftc.gov/system/files/documents/cases/140724lakshmiorder.pdf; *FTC v. PCCare247 Inc.*, No. 12-civ-7189, *available at* www.ftc.gov/system/files/documents/cases/140724pccare247order.pdf.

[9] *FTC v. Inbound Call Experts, LLC*, No. 14-81395-CIV-81395 (S.D. Fla. November 14, 2014), *available at* www.ftc.gov/system/files/documents/cases/141119vastboosttro.pdf; *FTC v. Boost Software, Inc.* No. 14-CIV-81397 (S.D. Fla. November 12, 2014), *available at* www.ftc.gov/system/files/documents/cases/141119icetro.pdf; *FTC v. Pairsys, Inc.*, No. 1:14-civ-1192 (N.D.N.Y. September 30, 2014), *available at* www.ftc.gov/system/files/documents/cases/141024pairsyscmpt.pdf.

[10] *FTC v. Pairsys, Inc.*, No. 1:14-civ-1192 (N.D.N.Y. July 21, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3099/pairsys-inc.

[11] *See* Press Release, FTC Obtains Court Orders Temporarily Shutting Down Massive Tech Support Scams, November 19, 2014, *available at* www.ftc.gov/news-events/press-releases/2014/11/ftc-obtains-court-orders-temporarily-shutting-down-massive-tech; *see also FTC v. Inbound Call Experts, LLC*, No. 14-81395-CIV-81395 (S.D. Fla. November 14, 2014), *available at* www.ftc.gov/system/files/documents/cases/141119vastboosttro.pdf; *FTC v. Boost Software, Inc.*; No. 14-CIV-81397 (S.D. Fla. November 12, 2014), *available at* www.ftc.gov/system/files/documents/cases/141119icetro.pdf.

III. FTC Outreach

A. Foreign Law Enforcement

As noted above, our law enforcement experience indicates that many tech support scams originate from call centers located in India. Unfortunately, enforcing judgments against defendants located outside the United States presents challenges. As a result, the FTC has been actively working with government officials, law enforcement, private companies, and trade associations in India to combat this problem at the source.

In July 2014, the FTC sponsored a roundtable in New Delhi to develop a long-term strategy for combatting various types of telemarketing fraud originating in India, including tech support scams. The roundtable brought together Indian and foreign law enforcement officials, as well as representatives from India's legitimate call center industry, technology companies, and consumer groups. The Canadian Radio-television and Telecommunications Commission and the United Kingdom's National Crime Agency also participated. The meeting ultimately led to formation of a council of industry leaders and government officials dedicated to combatting Indian telemarketing fraud and development of an action plan to address the problem.

One year later, in September 2015, the FTC held a follow-up conference in New Delhi that continued last year's work and focused on assisting Indian law enforcement to prosecute known telemarketing scammers operating in India. That conference focused on using banking data to identify scammers, improving processes for sharing information with Indian law enforcement about perpetrators of telemarketing scams, and developing methods to assist Indian law enforcement investigations. The FTC also has had discussions with India's telecommunications regulator – the Telecom Regulatory Authority of India – to explore options

for preventing Indian telemarketing fraudsters from gaining access to the necessary infrastructure to place calls to American consumers.

Through the two conferences and numerous follow-up discussions, the FTC has developed relationships with public and private sector partners in India to help fight tech support scams at their source. The agency also has laid the foundation to encourage and assist Indian law enforcement in taking action against Indian telemarketing fraudsters.

In addition, the FTC has strong working relationships with law enforcement partners in other countries that have been targeted by this scam, including Canada, the United Kingdom, Ireland, Australia and New Zealand. FTC staff has worked with them on investigations and litigation, and we are together engaged in proactively combatting tech support scams that affect millions of consumers worldwide. We also work closely with our foreign partners all over the globe through the London Action Plan, an international public-private cybersecurity enforcement network. Combatting tech support scams through international cooperation remains a top priority.

B. Consumer Education and Industry Outreach

The FTC has an active campaign to increase consumers' awareness of tech support scams. The agency is spreading the word to consumers about tech support scams through information posted on the FTC's website (www.consumer.ftc.gov), including blog posts and videos.[12] Consumers have viewed the FTC's articles and blog posts about tech support scams

---

[12] Some examples of FTC consumer outreach concerning tech support scams may be found at:

- www.onguardonline.gov/articles/0346-tech-support-scams www.onguardonline.gov
- www.consumer.ftc.gov/articles/0346-tech-support-scams
- www.consumer.ftc.gov/blog/getting-your-money-back-after-tech-support-scam

more than half a million times in the last year, and consumers have submitted hundreds of blog comments about these scams. Moreover, the agency is in the process of creating a new video on tech support scams.

In addition to its outreach specifically concerning tech support scams, the FTC created Pass It On last year, an innovative education effort aimed at active, older adults. Pass It On encourages seniors who learn about various scams to pass the information on to family and friends who might need it.[13] The Commission also entered into an innovative program with the AARP Foundation in 2012. As part of the program, the FTC refers for individual peer counseling consumers over age 60 who have called the FTC's Consumer Response Center to complain about fraud, including impostor fraud such as tech support scams.[14] The counseling provides older Americans with important support to help overcome the non-monetary impacts of being targeted by fraudsters. In the last six months, the FTC has referred over 1,000 consumers to AARP. In 2014, the AARP Foundation peer counselors successfully communicated with more than 1,400 people referred by the FTC, providing one-on-one advice and guidance to consumers to help them avoid future fraud.[15]

- www.ftc.gov/news-events/blogs/business-blog/2012/10/boiling-point-about-tech-support-boiler-rooms
- www.consumer.ftc.gov/blog/tech-support-scams-part-2
- www.consumer.ftc.gov/blog/ftc-combats-tech-support-scams

A recording and transcript of part of a scam call are available at: www.ftc.gov/news-events/audio-video/video/tech-support-scam-undercover-investigation.

[13] www.ftc.gov/PassItOn.

[14] The FTC only refers consumers who have consented to being contacted by the AARP.

[15] The consumers contacted by the Foundation counselors reported having lost nearly $19.5 million.

The Commission also regularly communicates and cooperates with legitimate companies in the computer industry and receives investigative assistance from industry partners. In one collaborative initiative, for example, the FTC held a workshop on how "Fraud Affects Every Community." The workshop brought together consumer advocates, state and federal regulators, fraud prevention experts, industry members, and academics to explore frauds – including tech support scams – that affect vulnerable groups, including older adults.[16]

IV. Conclusion

The FTC will continue its multifaceted approach of: (1) bringing law enforcement actions against scam operators who take advantage of consumers' fears and vulnerability to sell worthless services and products; (2) working with our international law enforcement partners; and (3) educating consumers and working with legitimate industry to combat this problem.

Thank you for the opportunity to share some of the FTC's work in the battle against tech support scammers. We look forward to working with the Committee on this important issue.

---

[16] Press Release, Commission Announces Workshop to Explore How Fraud Affects Different Communities (Sept. 9, 2014), *available at* https://www.ftc.gov/news-events/press-releases/2014/09/commission-announces-workshop-explore-how-fraud-affects-different.

Written Testimony of David Finn

Associate General Counsel and Executive Director, Microsoft Digital Crimes Unit

Before the Senate Special Committee on Aging on "Virtual Victims: When Computer Tech Support Becomes a Scam"

Biography: As Executive Director and Associate General Counsel of the Microsoft Digital Crimes Unit, David Finn leads a team of approximately 100 people, composed of former prosecutors, law enforcement officials, investigators, intelligence analysts, Big Data specialists, paralegals, business professionals, security analysts, and attorneys – located in more than 30 countries around the world – and oversees the company's global enforcement and intelligence efforts against organized criminals and other illicit organizations engaged in all forms of cybercrime. He has collaborated extensively with prosecutors and law enforcement officials worldwide since joining Microsoft in 1999.

Before working at Microsoft, David was an Assistant United States Attorney in New York City, where he worked closely with various U.S. federal and state law enforcement agencies and prosecuted an array of violent and economic crimes before juries and district court judges, arguing a dozen cases before the United States Court of Appeals for the 2nd Circuit.

A graduate of Harvard College and Harvard Law School, David is based at the Microsoft Cybercrime Center in Redmond, Washington, and lives in Seattle with his wife and two children.

I. Introduction

Chairman Collins, Ranking Member McCaskill, and members of the Committee, thank you for the opportunity to appear today at this important hearing. My name is David Finn, and I am Associate General Counsel and Executive Director of the Digital Crimes Unit at Microsoft.

My testimony today focuses on technical support scams, perhaps the single largest consumer fraud perpetrated in America today, victimizing an estimated 3.3 million people a year -- many of them senior citizens -- at an annual cost of $1.5 billion. This translates to a victim nearly every 10 seconds, with an average loss of $454 per consumer.

In addition to explaining this massive ongoing fraud and how it is perpetrated, I would like to take this opportunity to publicly thank the Federal Trade Commission, the Federal Bureau of Investigation, the state Attorneys General, local law enforcement, and senior advocacy groups such as AARP's Fraud Watch Network program for their efforts and partnership with Microsoft. We are grateful for their commitment to taking the strong, concerted action necessary to combat these nefarious scams and better protect seniors and other computer users across the country.

II. Technical Support Scams and How They Work

The technology industry has seen a surge in cybercriminals targeting individuals through technical support scams. These fraudsters contact consumers through a variety of methods: cold-calling,

Internet search engine advertising, web browser pop-ups, and spam email messages. Their goal is simple: sell unnecessary tech support for a non-existent problem and steal the victim's hard-earned money.

Scope of the Problem: Since May 2014, Microsoft alone has received over 180,000 tech support customer complaints. But we know these complaints are merely the tip of the iceberg. Customers of other software companies are also being victimized, and many victims are never even aware that they have been scammed. Fraudsters are stealing billions of dollars from consumers in what we believe to be the single most pervasive and fastest growing consumer fraud in the United States. Typical harm to a consumer includes:

- Loss of funds: $150 - $800 paid to scammers to "clean" their computer. In addition, scammers often enroll victims in an unneeded subscription service, which means the victimization is ongoing and continuous.
- Installation of malware with viruses, spyware, adware, keystroke loggers, and other harmful applications.
- Theft of personal identity information during remote access to "fix" the consumer's computer.

How the Scams Work: The objective of technical support scams is to deceive consumers into believing their computer suffers from malware or other technical issues. Scammers often cold call their victims, using lists of individuals available for sale on criminal web forums. Scammers also set up websites that cause a consumer's computer to become completely unresponsive; an alert will appear warning the victim that assistance is required to "clean" the machine and directs the victim to call the tech support scam company for help.

But regardless of how the scammers make contact, the key is to get potential victims on the telephone. Once a victim is on the phone, scammers gain the victim's trust by claiming they work for Microsoft or another reputable company. The scammers then manipulate the victim into granting remote access to the victim's computer, where they confuse the person into believing that the computer is infected with viruses or malware. For example, during our investigation we called scam support companies, where we saw first-hand how they bamboozle the user. Without ever running a scan, the support agents took control of the computer and typed and circled in red on the screen that "viruses" infected the computer, "unwanted people" were trying to "steal" information, "Russian connections" were made, and hackers were trying to access the machine – all a complete and utter fabrication by the scammer. Having aroused the consumer's fears, the fraudster then sells an unneeded service to fix a non-existent problem.

These schemes are often directed by individuals and organizations with a physical presence in the United States, but they frequently rely on the resources of call centers located abroad. While the vast majority of call centers operate legally and are not associated with technical support fraud, we have found that, in most cases, the fraudulent support calls themselves appear to originate from call centers located overseas.

Who is Being Targeted: Cybercriminals typically victimize the most vulnerable people that they can find and, in the case of technical support scams, this is often seniors. According to the Federal Bureau of Investigation, senior citizens are being targeted by fraudsters for the following reasons:

- Seniors are most likely to have a "nest egg," own their home and have excellent credit—all of which makes them attractive to con artists. People who grew up in the 1920s, '30s, and '40s were generally raised to be polite and trusting. Con artists exploit these traits, knowing that it is difficult or impossible for these individuals to say "no" or just hang up the telephone.
- Seniors are less likely to report a fraud because they don't know whom to report it to, are too ashamed at having been scammed, or don't know they have been scammed.
- When older victims do report the crime, they may not be conversant in the technical terms necessary to explain how they fell victim to the scam. Con artists also know the effects of age on memory, and count on older victims not being able to supply enough detailed information to investigators.
- With limited mobility, seniors are far more likely to rely on online services for an increasing array of services and as a connection to the "outside world." This makes them even more susceptible to cyber scams.

If You Are a Victim: If a consumer believes that they have been victimized by a technical support scam, they should immediately take the following actions to protect their computer, online accounts, and finances:

- Report the scam to the proper law enforcement authorities and other groups, such as
  - State Attorneys General: naag.org/current-attorneys-general
  - Federal Trade Commission: ftccomplaintassistant.gov
  - FBI: www.ic3.gov
  - Better Business Bureau: bbb.org
  - Microsoft: support.microsoft.com/reportascam
- Run an anti-virus program to scan the computer for harmful software. If a consumer has downloaded or clicked on anything that might infect their system, then they should run a full anti-virus scan and remove all suspicious items. Consumers can also take their computer to an authorized repair center.
- Contact bank and credit card companies. If a consumer has disclosed any payment or personal information to the scammers, they should contact their financial institutions to obtain new cards and have alerts for fraudulent activity placed on their bank accounts.
- Contact credit agencies and visit the FTC's identity theft website at consumer.ftc.gov/features/feature-0014-identity-theft. Consumers should place a fraud alert with any one of the three major credit bureaus to signal to potential creditors that they could have been a victim of credit card or identity theft.
- Update passwords, including email, financial, retail, and social media accounts. If a consumer is concerned that any of their accounts are compromised they should make sure to change their passwords immediately.

III. Microsoft's Efforts to Assist Consumers and Combat the Scammers

In an effort to help protect seniors from technical support scams, our Digital Crimes Unit has a team of attorneys, investigators, data analysts, and business professionals diligently collecting data from customer-generated leads and working with the FTC, state Attorneys General Offices, and others in state and federal law enforcement. Specifically:

- Microsoft constantly reviews and screens ads using both automated and manual methods. Using big data analytics, Microsoft routinely blocks certain advertisers and domains from ever even publishing technical support ads. For those ads that do get through our review process, by cross-referencing information from customer complaints with specific ads and advertisers, we have been able to remove numerous fraudulent ads from our Bing platform.
- Microsoft's Digital Crimes Unit continues to work hand-in-hand with other divisions of Microsoft – our Customer Support Services group, Stores, and Answer Desk to better respond to customer concerns and victim complaints.
- Microsoft is collaborating with partners, such as the AARP, in an effort to stop fraudsters from continuing to target our customers with technical support scams.

Case Development and Legal Actions

Over the past year, Microsoft's Digital Crimes Unit has amassed the following information:

- Identified over 250 targets engaged in fraudulent technical support scam activity in the U.S.
- Performed detailed investigations into technical support scam enterprises.
- Secured evidence against the largest fraudulent technical support companies operating today.
- Collected technical support scam complaints from victims, broken down by city and state.

In December 2014, Microsoft filed a federal lawsuit against the most complained about technical support scam company in the U.S. – Omnitech/Consumer Focus Services (CFS). In addition:

- Microsoft has made case referrals to multiple state Attorneys General (AG) Offices, including detailed referrals and reports to AG Offices in Washington, Illinois, Massachusetts, New Hampshire, and Utah.
- The Florida Attorney General filed four enforcement actions against technical support scammers and Microsoft provided crucial assistance against one of the defendants.
- Microsoft launched a company-wide partnership with AARP to help educate seniors about online safety.
- The FTC took numerous enforcement actions against technical support scammers, including several matters in which Microsoft supplied evidence, and launched a consumer education website.

Microsoft/State Attorneys General Partnership

Microsoft has been diligently pursuing fraudsters who prey online with new and evolving scams, but there is a limit to what one company alone can accomplish.

In the wake of new and increasing scams, the state AGs have become very active. Their offices are now seeing what the experts at Microsoft have seen—an explosion in the numbers of technical support scam complaints and too few resources and technical expertise to pursue the most egregious scammers.

Microsoft welcomes the opportunity to work with state AGs on both consumer protection and criminal enforcement actions, perhaps even through a multi-state action, to deter and bring to justice technical support scammers. Such a public-private effort combines the required technical expertise to investigate technical support scam cases with the leadership, legal authority, and regulatory might that state AGs can bring to the problem.

Microsoft's Cooperation with Federal Law Enforcement Agencies

Recently, members of my team in the Digital Crimes Unit and I met with James Trainor, Assistant Director of the FBI Cyber Division, along with top members of his Cyber Division team. We discussed several important security issues, including those surrounding these technical support scams. Assistant Director Trainor pledged his support and commitment to work with Microsoft on these matters, and noted that the FBI recently stood up a Field Office to target cybercriminals, including fraudsters like the ones behind these scams. We very much appreciate Assistant Director Trainor's support, and we are now working closely with the FBI on a number of cases. We are confident that the FBI's leadership and commitment will lead to concrete and meaningful enforcement action.

Microsoft has also supported the FTC's efforts to put technical support fraudsters out of business. Since 2012, the FTC has exercised its broad powers and filed a number of cases. Microsoft has provided documentary evidence and sworn testimony in many of those cases, and helped Commission staff to better understand some of the technical details involved in the scams. Additionally, we have collaborated with the FTC to help raise awareness of the problem though public events, most recently in a June 2015 discussion in the Microsoft Washington DC office on Combating Tech Support Scams.

We have also worked closely with the FTC as part of our strategy to extend enforcement to overseas call centers behind many of the technical support scams. As part of our collaboration with the FTC, Microsoft participated in a meeting in Dublin, Ireland, on June 8-11, 2015, where we met with international partners and spoke on a panel entitled "Coordinating with Criminal Enforcement Agencies." Following that event, on September 9, 2015, Microsoft, again with the assistance of the FTC, convened a Call Center Fraud Roundtable that included Indian law enforcement in New Delhi, India. Microsoft presented detailed information about our investigations and the central role that overseas call centers play in perpetuating these scams. Law enforcement attendees reacted positively to our case work, pledging to collaborate closely with us and take concrete action against overseas-based targets.

We thank the FTC and the federal law enforcement agencies for their assistance, and their ongoing efforts to reach out to law enforcement officials overseas to crack down on the illegal and fraudulent scams that some of these call centers facilitate.

Finally, Microsoft has worked closely with law enforcement in the UK, identifying technical support scam targets there. A number of joint investigations are now underway in the UK.

Collaboration with AARP

In the Spring of 2015, Microsoft collaborated with AARP Washington to develop a series of "Scam Jams" focusing on online safety for seniors. These educational half-day events, open to seniors around Washington State (Seattle, Spokane, Redmond, Kennewick, and Yakima) were designed to educate senior citizens and their adult children about staying safe online. The largest of these events occurred on the Microsoft campus, featuring several Microsoft senior leaders as well as Frank Abagnale, renowned con-artist-turned-FBI-agent, who is featured in the movie "Catch Me If You Can."

The purpose of these events was to address the growing problem of online scams that are directed at Microsoft's senior customers by arming seniors with education and best practices to spot scams, use security software, and otherwise stay safe online. Further, Microsoft provided information about safety features built into Microsoft products and services.

Each event drew roughly 300 attendees, signifying that online safety is an important topic among AARP members. In fact, at every event, seniors stayed for an hour or more after the program had ended to take the opportunity to speak with representatives from Microsoft, and to ask more questions. Based on positive feedback received from the Microsoft AARP Scam Jams, Microsoft and AARP's national Fraud Watch Network have decided to expand the partnership beyond Washington to other states.

Recommendations and Next Steps

At the heart of the technical support scam problem lie three straightforward facts. First, as of now, there is simply too much money being made by cyber scammers, and too little chance of their being caught and punished, to establish the deterrence that people deserve. Second, education is an important part of preventing future consumer harm, but education alone will not alone be enough. Third, while we have sufficient laws on the books to punish fraudsters both criminally and civilly, we need concrete enforcement action to reign in this conduct, requiring strong cooperation across state, federal, and international agencies, and close partnership with private industry.

Accordingly, we would recommend this Committee take the following actions to assist in this effort:

A. Request that the relevant federal agencies monitor the problem and implement the best mechanisms to identify and eradicate these scams including the creation of a FTC-DOJ Tech Scam task force as a comprehensive means to address these scams.

B. Propose interagency coordination with the State Department and other relevant agencies to ensure that law enforcement officials overseas are taking concrete action, and prosecuting the call centers that perpetrate these frauds on U.S. citizens.

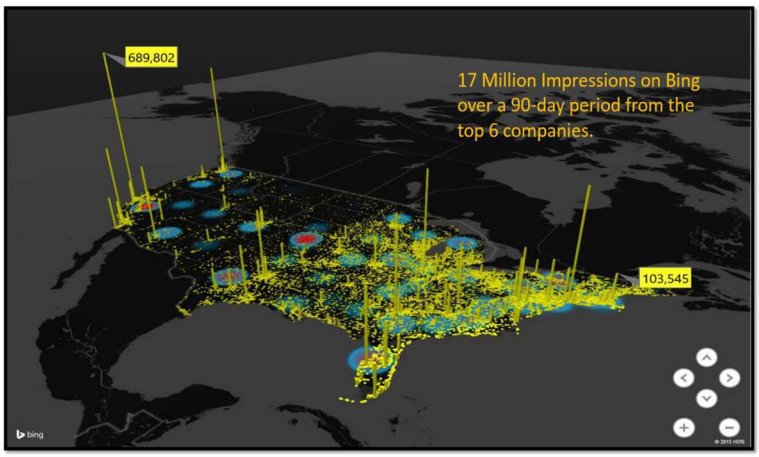
C. Support and encourage the state Attorneys General as they continue their work to hold technical support scammers accountable through their broad consumer protection authority.

D. Continue the Committee's oversight of this issue – which Microsoft believes is the largest ongoing fraud in the U.S. – to ensure that government and industry are making progress fighting these fraudsters.

Thank you for the opportunity to testify, and I look forward to answering your questions.

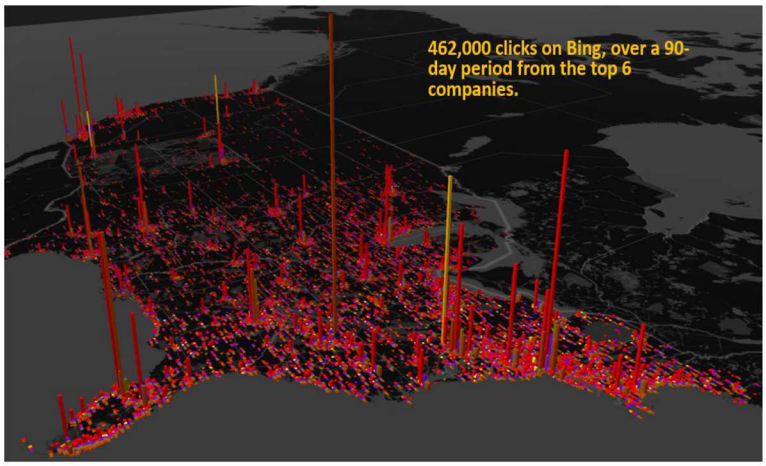
Appendix

Impact of Tech Support Scams



The above chart shows the number of impressions on Bing alone over a 90-day period from the top 6 scammers. An impression represents the search results from Bing that populate with advertisements for these top 6 tech support scammers.

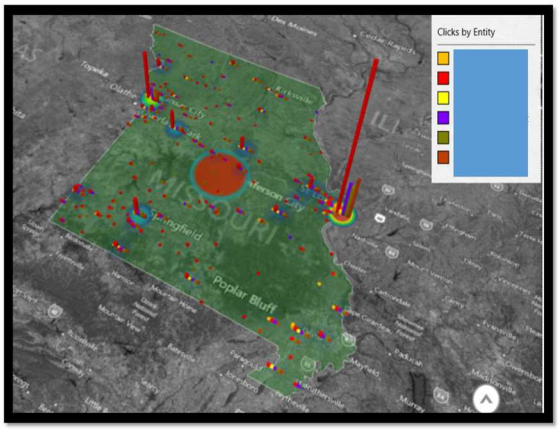
Victims Visiting Websites for Top 6 Targets



The above chart shows the number of clicks on Bing alone over a 90-day period. A click represents individuals who, having received an impression from a search query, clicks on that result and is taken to the website for one of the top 6 tech support scammers. While an impression could be seen as a potential victim of a scam, a click represents a much more likely victim, as they are interested enough in the search result to actually visit the website.

Missouri – Ad Clicks & Impressions over 90-day Period

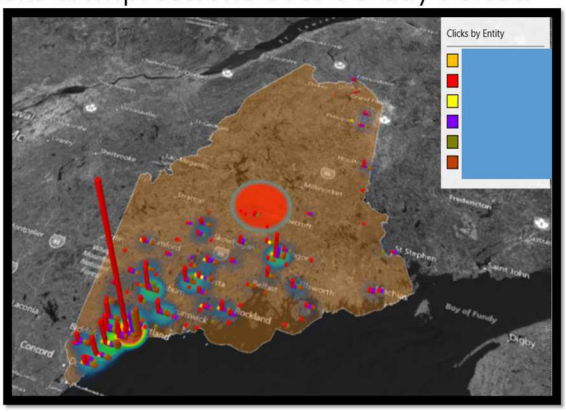
Total Clicks:
4,876
Total Impressions:
281,880



The above chart shows the combined clicks and impressions (described above) in Missouri alone over a 90-day period, once again on Bing.

Maine – Ad Clicks & Impressions over 90-day Period

Total Clicks:
1,299
Total Impressions:
75,266



The above chart shows the combined clicks and impressions (defined above) in Maine alone over a 90-day period, once again on Bing.

LSSM

PROVIDING QUALITY LEGAL AID

Prepared Statement Of
Legal Services of Southern Missouri
Lew Polivick, Deputy Director

Before The
United States Senate
Special Committee on Aging

On

Virtual Victims: When Computer Tech Support Becomes a Scam

Washington, DC
October 21, 2015

Chairman Collins, Ranking Member McCaskill, and Members of the Committee, I am Lew Polivick, Deputy Director of Legal Services of Southern Missouri. I appreciate the opportunity to share what our program is seeing and how we are trying to help victims of computer scams.

"The number one rule of thieves is that nothing is too small to steal."

Jimmy Breslin

The damage caused by consumer fraud is often magnified for the low income victim. Our low income clients are less educated than the population in general and they are often reluctant to contact law enforcement agencies about their problems, due to embarrassment or mistrust. Low income victims of consumer fraud frequently take longer to discover or report the crime. They don't obtain and review credit reports as often as more affluent citizens. This results a number of problems, including harassment by debt collectors and difficulty in getting credit reports corrected. Our older clients are often attractive targets for scammers hoping to take advantage diminished mental capacity or other health problems that make the victim more susceptible to manipulation.

LSSM provides free legal service in civil matters to low income citizens in 43 southern Missouri counties. The great majority of our clients have income less than 125% of the poverty line. In addition to providing legal advice and representation, LSSM also provides public education and outreach services to partnering agencies and community groups.

I. Recognizing the Problem

Computer tech support scams have been plaguing Missourians for several years. Scammers call a home posing as computer security pros from legitimate companies. They often ask for the consumer by name. The fake security expert claims to have discovered a virus on the

consumer's computer and offers to help solve the problem for a fee. The criminal then ask the consumer to perform a variety of tasks to help combat the bogus threat such as giving the thief remote access to the computer, tricking them into downloading malware, and asking for bank and credit card information. The scammer may also try to enroll the consumer in a worthless computer maintenance or warranty program or bill the consumer for fake services or services that are available for free.

Those deceived suffer financial loss including money taken from their bank and credit card accounts, compromised passwords and identity fraud. The victims are often reluctant to report that they have been taken due to embarrassment or confusion as to the proper agency to contact. In some cases the victim may not realize they have been scammed until long after the fact when they start getting collection calls from creditors they don't recognize or see accounts on their credit report that they do not recognize.

II. Combating The Problem

A. Consumer Fraud Task Force Of Southern Missouri

In order to stop scams like the computer tech scam, LSSM formed the Consumer Fraud Task Force of Southern Missouri in 2013. The purpose of the task force is to make the community aware of deceptive practices and provide tips and information to allow consumers to make informed decisions. Task force members include local law enforcement, the FBI, the Missouri Attorney General's office, the Federal Trade Commission, the US Postal Inspector and the Better Business Bureau.

The task force meets at least quarterly and serves as a link to various agencies to provide updated information on fraud and deceptive practices occurring in the region. Task force members take the information they learn at the meetings and pass it along to their staff and

partner agencies. The information is also shared with the public through press releases coordinated by the task force.

B. Community Outreach

Since 2013, LSSM has presented several outreach programs about consumer fraud, sometimes referred to as Scam Schools. We partner with local senior citizen centers, health care providers, the University of Missouri Extension Service and others to organize these programs. The latest scam variations are discussed at the classes as well as information about discovering and reporting scams and working with various agencies to stop them. These programs are well attended and allow us to provide consumer fraud information directly to more than 300 people per year.

Persons attending our outreach programs are encouraged to share information about scams with their family and friends and to watch for signs that someone they know may be a victim. LSSM makes a special effort each March to visit senior centers to provide information on current scams as part of National Consumer Protection Week.

LSSM regularly posts scam alerts on our web site, LSOSM.ORG, which receives thousands of contacts annually. We annually distribute hundreds of educational brochures relating to consumer fraud in our five offices and at outreach programs throughout southern Missouri.

III. Repairing The Damage

Victims of tech scams often suffer losses including money paid to the scammer as a fee or taken from their bank or credit card accounts, compromised passwords and identity theft. Recovering money directly from the scammer is not an option because the scammer's identity is

rarely known. The services provided by LSSM vary depending on the degree of damage done by the scammers. Generally, the victim is advised to:

- Use legitimate security software to run a scan and see if there is malware or virus activity on their computer.
- If they gave the caller any passwords, change them for the account in question and any other accounts for which they use the same passwords.
- If the caller charged for services to the victim's credit card, call the card company and insist that those charges be reversed.
- If personal financial information may have been stolen, order a credit report.

If the victim's credit report shows suspicious activity, LSSM will assist the client in filing an initial fraud alert with the credit reporting agency. This will help stop a scammer from opening new credit accounts in the victim's name. The initial fraud alert will stay on the victim's credit report for 90 days.

If the stolen information is used by the scammer to open a credit account or access existing accounts, the victim is advised to contact the police, and to file a complaint with the Federal Trade Commission.

A. Defense of Collection Suits

In cases where the scammers are successful in getting false credit cards issued, LSSM provides legal representation to stop harassment by debt collectors and defend debt collection suits filed against the scam victim. LSSM's attorneys are usually successful in getting such suits dismissed by the creditor once they provide documentation that the scam victim reported their identity theft to the police, attorney general or FTC.

B. Filing Identity Theft Reports

Scam victims often contact LSSM out of frustration after they have tried to unsuccessfully to fix the problems on their credit reports. LSSM assists by helping them gather supporting documents needed to get an Identity Theft Report accepted by the three major credit reporting agencies - Equifax, Experian and TransUnion. The Fair Credit Reporting Act states that a credit reporting agency must block the fraudulent information the victim has identified within four business days after accepting the victim's Identity Theft Report. When it accepts the Identity Theft Report, the credit reporting agency also must notify the furnishers of the fraudulent information that it is blocking the information that they furnished.

C. Private Bar Assistance

Because of their experience in this area, LSSM attorneys are often contacted by members of the private bar for assistance with forms, research materials and other information relating to consumer fraud. LSSM works closely with attorneys throughout southern Missouri to combat consumer fraud.

IV. Future efforts

LSSM is constantly adapting its program to meet the legal needs of low income citizens. Providing qualified attorneys and staff to give legal advice and representation to victims of crimes such as computer tech support scams is a high priority. When it comes to consumer fraud, an ounce of prevention is worth well more than a pound of cure. For that reason we will continue to expand on education efforts such as the Consumer Fraud Task Force to try to eliminate these scams in southern Missouri.

Thank you again for the opportunity to appear before you today to discuss our efforts to combat consumer fraud scams which target the low income and senior citizens of Missouri.

Statements for the Record

March 10, 2014

113 New Island Ave.
Peaks Island, ME 04108
(207)766-5879
fsisland@aol.com

RE: Complaint of Telemarketing/Computer Fraud

To whom it may concern:

In October and December 2013 I paid about $1,433 for what soon became evident as a completely bogus and fraudulent deal. While extremely embarrassed by my stupidity in having been taken by this, the continued and persistent phone calls from the perpetrators of this and concern for their apparent ability to further victimize me and others has prompted me to document and distribute the following and attached information.

I'm asking that you forward it to whomever may have an interest in curtailing their efforts, and/or to review it for any information that may be helpful in doing so. I will gladly provide any other information or access that I can to assist, and certainly authorize any legal actions that may be possible against them. I will gladly provide information to anyone you'd refer to me.

Of course I realize that any chance of financial recovery is near zero. But in typical victim fashion I am 66 years old, living on social security, no computer whiz, and am amazed at the brazen gall of these lying thieves. So I appreciate anything you might do to put an end to their dirty business. Thank you.

Sincerely,

Frank Schiller

attach: Chronology of fraud and computer page prints

Distribution: Portland ME Police Department
Maine Attorney General
Maine State Police Computer Crimes Unit
Federal Trade Commission

I would like to thank you for your time and trust which you have given to us. To protect you from fraud companies we will provide you your unique membership code:

Membership Code :- "MTSUK-786"

I would also like to confirm you that whenever you want any help from me please don't hesitate to write me at my direct email.

Email ID :- services@globalwebsupport.net / managermikewilliam@gmail.com

If you need more claraification on the information shared you can be reached at my direct line: +1-714-795-3200

Your Satisfaction is my motto...

Thanks & Regards

Mike William
Manager - Technical Team
Global Web Support

Re: Software purchased 10/13.