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.

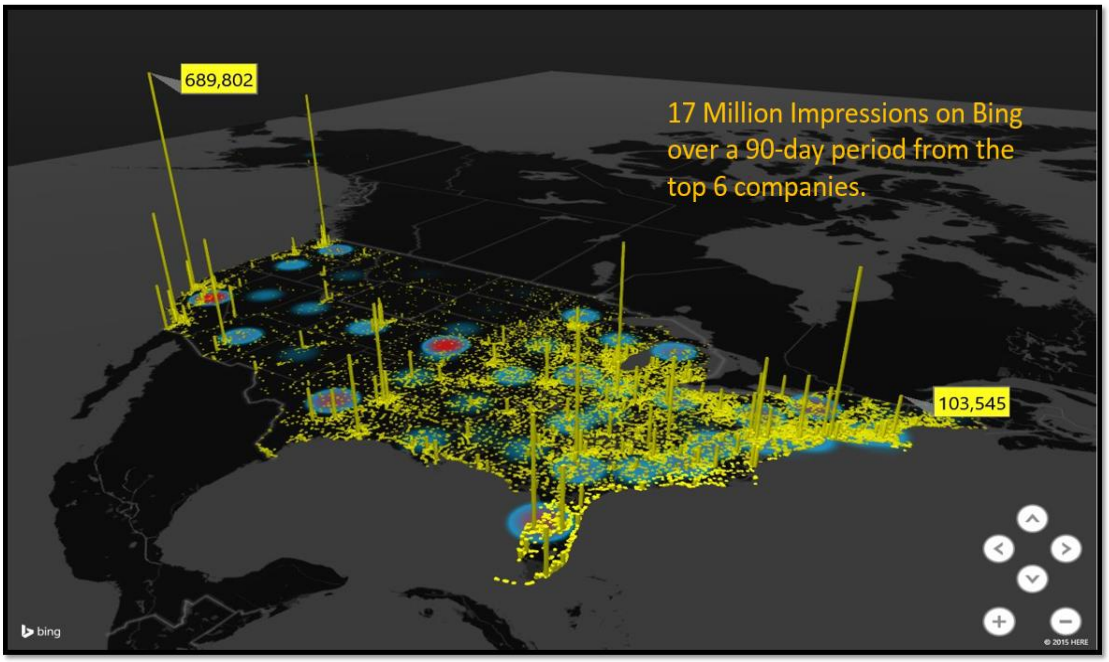
C. Support and encourage the state Attorneys General as they continue their work to hold technical support scammers accountable through their broad consumer protection authority.

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.

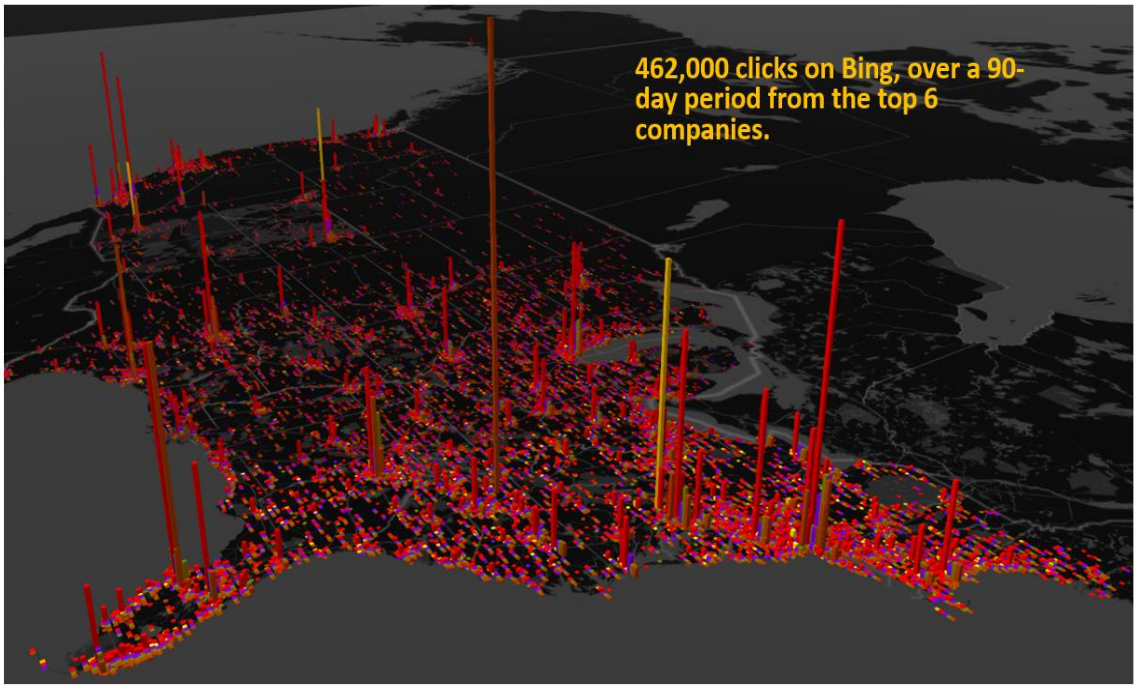
Appendix

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

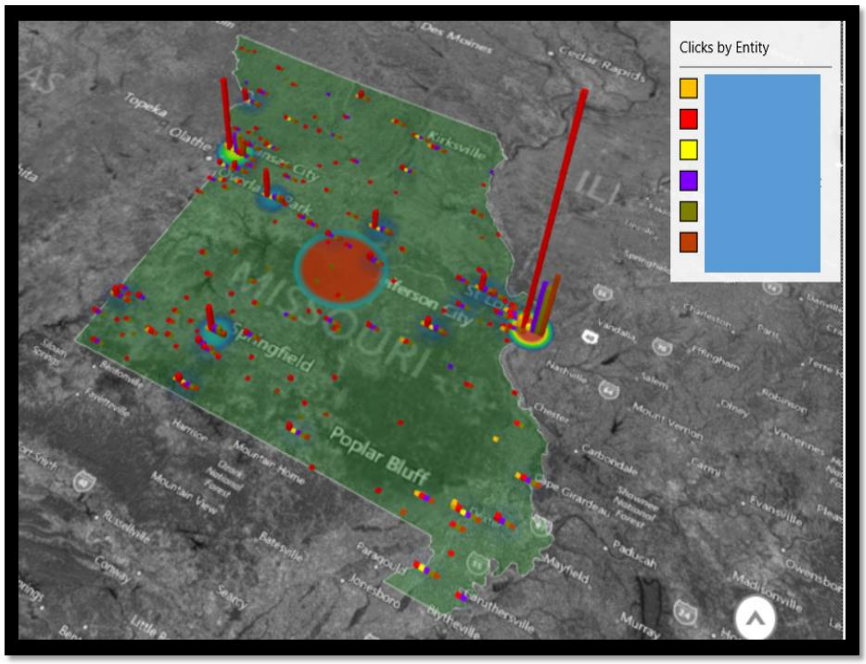


The above chart shows the number of clicks on Bing alone over a 90-day period. A click represents individuals who, having received an impression from a search query, clicks on that result and is taken to the website for one of the top 6 tech support scammers. While an impression could be seen as a potential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

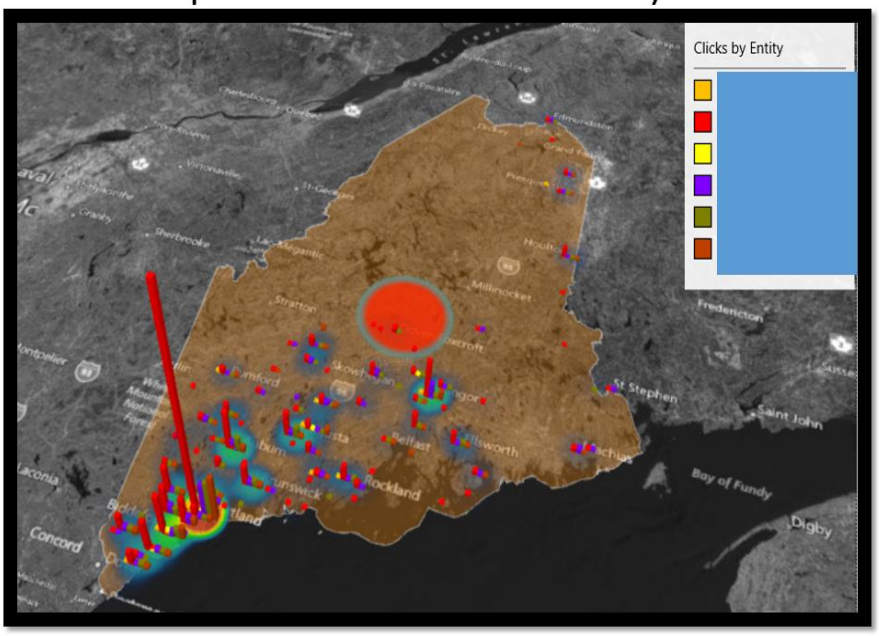


The above chart shows the combined clicks and impressions (described above) in Missouri alone over a 90-day period, once again on Bing.

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.