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.