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.