

Written Testimony of Detective Jason Moore
Auburn Maine Police Department

United States Senate Special Committee on Aging
Catch Me If You Can: The IRS Impersonation Scam and the Government's Response
Wednesday April 15, 2015, 1:30 p.m., Dirksen Senate Office Building, Room SD-562

Chairman Collins, Ranking Member McCaskill, and Members of the Committee, thank you for the opportunity to testify today about an IRS Impostor scam that I recently investigated. I am currently employed as a detective with the Auburn, Maine police department. I was hired in 1998 as a patrolman and was promoted to detective in 2006. I am here today to discuss a case I was assigned on Monday, March 23, 2015. The case involves a fifty-year-old woman who had been scammed out of \$23,000 by someone posing as an IRS agent.

The victim of this crime is very embarrassed and has requested anonymity. Accordingly, I will refer to her as Mrs. A for the purpose of this testimony.

On Saturday morning, March 21, 2015, Mrs. A came into the Auburn Police Department to report that she felt she may have been scammed. Officer Ham was dispatched and met with her. She explained to him that on Thursday, March 19, 2015, she had received a message on her home answering machine. The message did not address her by name, and simply stated that she was being sued by the IRS. A phone number of (202) 602-1339 was provided for her to call back.

She returned the call and spoke to a man with an Indian-sounding accent who stated his name was Alex Rogers. He identified himself as an agent with the IRS and provided badge number 101895337. He stated that he was calling regarding a tax audit because Mrs. A had used the wrong tax rate when she filed her taxes. He alleged that three attempts had been made to speak with her in person at her residence, but no one was home. He went on to provide dates for these attempts. September 25, October 29, and November, 23, 2014.

Mr. Rogers told Mrs. A that this issue was very serious, and was now in the hands of the courts. He told her that an arrest warrant had been issued for her, and liens would be put on her home and vehicle. He said that she owed \$4,982 to cover the tax liability for the years 2008-2012, and that if it was not paid by 5:00 pm that day the lawsuit would go through and she would be taken into custody.

Mrs. A explained that she had her grandchildren and would be unable to pay that day. Mr. Rogers told her that was no reason, and that they would still come arrest her. He also told her that she could not tell anyone that she had been contacted by the IRS—including her husband.

Mrs. A said that she was very nervous and shaking at this point. She questioned why she had not been previously notified by the IRS and why the IRS had not sent her a letter. Mr. Rogers said that due to the seriousness of the matter, the papers had to be hand delivered.

Following Mr. Rogers instructions, Mrs. A went to her bank and withdrew cash, and then she went to a WalMart and purchased MoneyGrams that transferred funds directly to a prepaid Pay Power card. She was told to buy them using a different sender name for each MoneyGram. These were predominantly in \$500 increments.

She was then sent to the nearest Bank of America branch, which is in Brunswick (about 30 minutes away) and was instructed to wire funds to a specific account. There was a technical issue which prevented the wire transfer. At this point the scammers sent Mrs. A to the Brunswick WalMart to purchase more MoneyGrams. At 6:00pm Mr. Rogers told Mrs. A that the IRS office was closed and the legal action would be put on hold until 9:00am the following day, Friday, March 20, 2015.

Throughout this ordeal, Mrs. A was told to stay on the phone. She was continually threatened with arrest if she told anyone that she was in contact with the IRS or failed to make payments as instructed. On a couple of occasions she lost connection. She then received a phone call from (207) 333-6650, which is the number of the Auburn Police Department. She spoke with a person who claimed to be Lt. Green (there is no one employed at the Auburn Police Department with the surname of Green). He told her that she would be arrested if she continued to hang up. She explained that these were unintentional dropped calls. Lt. Green said that he would fax a note to Mr. Rogers explaining this. When she reconnected with Mr. Rogers, Mrs. A inquired if he had received the fax from Lt. Green. He said that he did. This police impostor, using a spoofed police number, and supposedly sending faxes to Mr. Rogers made Mrs. A too fearful to not comply.

Throughout these events, Mrs. A had her two young grandchildren with her. She was in tears when she returned home, and was too scared to tell her family why she was distressed.

As promised, Mr. Rogers called back Friday morning. He was now claiming Mrs. A owed another \$7,432. He had her speak with two other people who were supposed to be with the IRS. One claimed to be an attorney, the other an account manager. They used the names Shawn Davis and Mike Walker.

Mrs. A was next sent back to Bank of America. She was given an account name (Devi Ji Inc.) and number. She made the \$7,432 deposit and scanned and emailed the receipt from the FedEx Office in Auburn, as instructed by Mr. Rogers. The email was addressed to jack.cooper.irs@gmail.com.

After completing that task, one of the phony attorneys told Mrs. A that they needed \$900 for document fees. She began to cry, and was told that if she continued to cry they would hang up and the process would start all over again. She was then told that they had discovered another \$14,322 that was due. They said that they would settle for \$10,500 and she would receive 40% of it back with her tax refund in three weeks.

Mrs. A was directed to return to Bank of America, and deposit \$5,000 into the aforementioned account, and \$5,500 into an account under the name Ammar Banatwala. She discovered the second account was closed, so she only made the \$5,000 deposit. She was then sent back to FedEx Office to scan and email the receipts. After that, she was told to destroy the receipts. The scammer wanted to hear her rip up the receipts over the phone. However, she tore up other papers instead.

Mrs. A was next directed to obtain \$6,300 in money orders from the Western Union at the Kmart store in Auburn. She purchased twelve \$500 money orders and one \$300 money order. She then sent them via FedEx overnight to a Days Inn in Greenwood, SC. The package was simply addressed to Andy.

Mrs. A was again continually threatened through the day.

The scammers told her that the IRS offices were closing for the weekend, and they would call her again Monday morning.

Upset by what had transpired, and becoming increasingly suspicious, Mrs. A went to the Auburn Police Department. She brought with her receipts for all of the transactions.

After I was assigned the case on Monday morning, I read Officer Ham's report, and was preparing to call Mrs. A, when I learned she was in the lobby of the police department.

I met with her and brought her into an interview room. When I first approached Mrs. A in the lobby, her mobile phone was ringing, but she did not answer it. As we walked to the interview room I noticed that her phone was ringing again, and she continued to ignore it. When we began to talk in the interview room, her phone rang once again. She said it was "them," which I took to mean the scammers.

I answered her phone and found myself speaking to a male with a heavy Indian accent. He asked to speak to Mrs. A, and I told him that he could not. I did not identify myself by name, but did allude to the fact I was with law enforcement. I made it known that the ruse was over and he would no longer be speaking with Mrs. A. The male persisted in his requests to speak with her, so I terminated the call.

Within seconds she received yet another call from the same number (202) 602-1339. I answered and informed the male that each time he called, he would be speaking with me. He persisted in

his requests to speak with Mrs.A. I continued to tell the man that he would not be speaking with her again. I was very firm and somewhat rude. The subject then terminated the call.

Mrs. A explained the calls have been near constant. She said that she received some calls from local numbers earlier that morning, but did not answer out of fear it was the scammers. She showed me the number, (207) 753-2500, which I immediately recognized to be the Androscoggin County District Attorney's Office (our local prosecutor).

Mrs. A told me that she had called the Days Inn and spoke to staff there. She said that they seemed familiar with Andy and believed his last name to be "Patel."

Mrs. A had also called Western Union and Pay Power to file fraud charges with them. (Pay Power is the provider for the pre-paid cards she loaded via MoneyGram at WalMart).

Pay Power told her that if I called they would be able to provide me with some more information. I did call, but the only thing they told me was that they were escalating the report to the next level of support, and they would get back to me in 3-5 days. After not hearing back from Pay Power, Mrs. A called them. She was told that her case was in resolution, and that they would be in touch with law enforcement.

Since Mrs. A made cash deposits at a Bank of America branch, I thought it was important that I notify them. I also wanted to inquire if there was a way to reverse the deposit since it was made as part of a fraud. It took several attempts for me to reach someone at Bank of America who could assist me. I eventually made contact with Ms. Chauntel James who is a Senior Investigator with the Fraud Investigations Group. I told Ms. James why I was calling and what assistance I was seeking.

Ms. James explained that she had already been assigned to look into that account due to suspicious activities. While I was explaining the details of my case, she noticed that there was an active wire transfer from the account in question, to an overseas account. Ms. James promptly ended the call so that she could turn her full attention to stopping the wire transfer.

Ms. James later advised me that Bank of America had been successful in halting the wire transfer. I understand from Ms. James that Bank of America was also able to recover money from victims in California and New Jersey totaling some \$34,000 that was also in the account in question. Bank of America has agreed to refund Mrs. A her \$12,432 and is in the process of doing so.

From speaking to Ms. James, I understand that if Mrs. A had torn up the receipts as instructed, she may not have been able to recover her money from Bank of America.

On behalf of Mrs. A I filled a complaint online with the Treasury Inspector General for Tax Administration. She received a phone call the next day from Special Agent Kris Rowlette.

Agent Rowlette told Mrs. A that he would be looking into the matter, and would contact the Days Inn in South Carolina. He asked her for copies of her receipts and statement. I emailed those to him on Mrs. A's behalf. In my email I advised Agent Rowlette of my involvement, and that I wouldn't take any further action until I spoke with him. He replied that he would contact me the following week. Due to conflicts we have been unable to speak directly yet. I am aware that he is actively working the case.

I and other detectives with whom I work have fielded calls from citizens who have received calls similar to the one Mrs. A did. I received one such message on my home phone while I was working on this case. I fear that there are other victims who have not reported crimes they have fallen victim to out of embarrassment, or who may be unaware that they were scammed.

The Auburn Police Department issued a press release warning the public of this crime. We have also talked about it in social media. I have warned my personal friends on social media as well.

I am hopeful that our public outreach will serve to minimize future victims of this crime. I am, however, dismayed that Mrs. A's large volume of money order and prepaid card purchases were unchallenged by the retailers or the money transfer providers. She has been given little hope of getting the remaining \$11,256 back from those businesses.

Transaction History

Thursday, March 19, 2015

MoneyGram/Pay Power (Auburn Wal-Mart)

12:26pm \$500

12:30pm \$499

MoneyGram/Pay Power (Brunswick Wal-Mart)

2:54pm \$499

2:57pm \$500

3:24pm \$499

3:37pm \$500

4:25pm \$499

4:28pm \$500

MoneyGram/Pay Power (Auburn Wal-Mart)

6:14pm \$460

6:17pm \$500

Friday, March 20, 2015

Bank of America

11:41am \$7,432 deposit

4:01pm \$5,000 deposit

Western Union (Kmart)

5:25pm 5x\$500 (\$2,500) money orders

5:26pm 7x\$500(\$3,500) money orders

5:26pm \$300 money order

FedEx Office

6:03pm Shipped Western Union money orders to South Carolina. Incurred \$59 charge.

The victim paid a \$3.95 for each MoneyGram/Pay Power transaction, and \$0.69 for Western Union transaction.

Detective Jason Moore
Written Testimony
Exhibit 1



Auburn Police Department



Phillip L. Crowell
Chief of Police

Jason D. Moen
Deputy Chief

Rita P. Beaudry
Exec. Assistant

FOR IMMEDIATE PRESS RELEASE

March 24, 2015

PHONE SCAMMERS USING SPOOFED GOVERNMENT NUMBERS

Auburn Police Department is conducting a fraud investigation where a local resident was defrauded out of several thousand dollars after falling victim to phone scammers. The victim received several phone calls from a male claiming to be an agent with the Internal Revenue Service Criminal Investigation Department. The male claimed to be investigating a taxes owed issue involving the victim. The male was quite rude and intimidating.

After hanging up on the male several times, the victim received two phones where the Caller I.D. information was spoofed to appear as though the calls originated from the Auburn Police Department's primary telephone number. She also received at least one phone call that was spoofed to appear as though that call came from the Androscoggin County District Attorney's Office main telephone line. Of course, these calls did not originate from this police department or the District Attorney's office; however, the victim found this scam was more believable due to these calls from local (spoofed) phone numbers. She did speak to a 'Lieutenant Green' (who, of course does not work for the APD) and this 'Lieutenant Green' threatened the victim with arrest by the Auburn Police Department if she hung up on the IRS. The victim was threatened repeatedly and was told to tell no one about this tax 'situation' or about the 'payments' she was making to the IRS.

Anytime you receive a phone call purported to be from the IRS, here's what to do:

- If you owe Federal taxes, or think you might owe taxes, hang up and call the IRS at 800-829-1040. IRS workers can help you with your payment questions.
- If you don't owe taxes, call and report the incident to Treasury Inspector General for Tax Administration at 800-366-4484.

If you have fallen victim to this type of scam, the IRS does have a website set up where victims of this type of 'IRS Impersonation Scam' can make a report. The URL is: http://www.treasury.gov/tigta/contact_report_scam.shtml

For More Information Contact:
Deputy Chief Jason Moen
207-333-6650 ext 2052

Detective Jason Moore
Written Testimony
Exhibit 2



Auburn (Maine) Police Department

FOR IMMEDIATE PRESS RELEASE

March 24, 2015

PHONE SCAMMERS USING SPOOFED GOVERNMENT NUMBERS

Auburn Police Department is conducting a fraud investigation where a local resident was defrauded out of several thousand dollars after falling victim to phone scammers. The victim received several phone calls from a male claiming to be an agent with the Internal Revenue Service Criminal Investigation Department. The male claimed to be investigating a taxes owed issue involving the victim. The male was quite rude and intimidating. After hanging up on the male several times, the victim received two phones where the Caller I.D. information was spoofed to appear as though the calls originated from the Auburn Police Department's primary telephone number. She also received at least one phone call that was spoofed to appear as though that call came from the Androscoggin County District Attorney's Office main telephone line. Of course, these calls did not originate from this police department or the District Attorney's office, however, the victim found this scam more believable due to these calls from local (spoofed) phone numbers. She did speak to a 'Lieutenant Green' (who, of course does not work for the APD) and this 'Lieutenant Green' threatened the victim with arrest by the Auburn Police Department if she hung up on the IRS. The victim was threatened repeatedly and was told to tell no one about this tax 'situation' or about the 'payments' she was making to the IRS.

Anytime you receive a phone call purported to be from the IRS, here's what to do:

- If you owe Federal taxes, or think you might owe taxes, hang up and call the IRS at 800-829-1040. IRS workers can help you with your payment questions.

- If you don't owe taxes, call and report the incident to Treasury Inspector General for Tax Administration at 800-366-4484.

If you have fallen victim to this type of scam, the IRS does have a website set up where victims of this type of IRS Impersonation Scam can make a report. The URL is: http://www.treasury.gov/tigta/contact_report_scam.shtml

Contact: IRS Impersonation Scam Reporting - U.S. Treasury Inspector General for Tax...

TIGTA, promoting integrity in the administration of internal revenue laws. The United States Treasury.

Treasury

Promoting it

Like Comment Share

Christopher Halford and 26 others like this.

47 shared

Daryl Smith WOW, this just shows that the general public needs to go back to school and learn something. My GOD, if someone threatens you over the phone and tells you to keep it a secret you have to think, SCAMMMMMMMMMM.

Betty Miles I got calls. But IRS, would never call, they send letters. Victims smarten up.

LaurieAnn Charest Thank you!

Lar Lar Meints I got called twice, I didn't answer and they left a message both times. I was basically threatened that a warrant would be ordered for my arrest. I informed my phone company and they took care of it. Never heard back and can't call that number.

Randy Perreault They called me and left a message, so I called them back and gave them a brief description of what I do for a living (fraud investigations). They hung up and now there line is busy. Lol

Gregg Lathrop How about stopping those calls from windows tech support. I asked them take me off their list and they said no we like to annoy you.

Bryan Kenney Kabe Kenney

NOTES

Do You Recognize This Alcohol Thief?

December 24, 2014

Can you identify these two shoplifting suspects?

August 31, 2014

A Hannaford Theft Suspect...

May 14, 2014

REVIEWS

4.2 ★ 4.2 of 5 stars • 43 reviews



Lisa Levesque — 5★

Like Comment



Kristopher Bouchard — 5★

Like Comment



Tell people what you think

APPS



Send a Tip



Commendations



iPhone & Android App

POSTS TO PAGE

Be the first to post on this page.

Write Post

Create Page

Recent

2015

2014

2013

2012

2011

2010

2009

Sponsored



100% U.S. Service
DiscoverCard.com
Talk to a real person any time
you call the dedicated
Discover #8 phone number



Liberty Mutual Insurance
welcome.libertymutual.com
Save Up To \$423* On Car
Insurance. 24/7 Claims
Assistance and more. Quote
Now!

Detective Jason Moore
Written Testimony
Exhibit 3



Jason Moore

March 25 at 4:55pm · Auburn, ME · 🌐 ▼

I'm sure many of you have heard about the IRS scam that's been going around. I am currently working a case with a resident who was scammed out of several thousand dollars. I, myself, received a voice mail today saying I was being sued by the IRS from (360)761-1115.

There seems to be a surge of these calls recently and I would urge you to not answer a call from any unrecognized numbers. These scammers are bold, persistent, and can also spoof their phone numbers to make them appear legitimate.

If you suspect you are being scammed, end the call and verify. No legitimate organization will object to this. A scammer will adamantly object.

Nobody expects to fall for these scams, but it can happen to anyone.

If you, or someone you know has fallen prey to this scam you can file a report at http://www.treasury.gov/tigta/contact_report_scam.shtml.

Please share this for exposure.



Contact: IRS Impersonation Scam Reporting - U.S. Treasury Inspector General for Tax...

TIGTA: promoting integrity in the administration of internal revenue laws. The United States Treasury...

TREASURY.GOV · @TIGTA.GOV

Like Comment Share

👍 Kim Gauthier Karlis, Cindy Anne, Steve Hammerton and 8 others like this.



Michelle L SJ Thank you for sharing Jason! I've shared!

March 25 at 6:22pm · Unlike · 👍 1



Eric Beaulieu We got a call like that a month ago. We didn't answer it

March 25 at 7:37pm · Like



Becky Tanguay 718-770-3538 & 636-754-3150, 206-687-9902. Denis had these 3 #s call him threatening him it could turn out badly if he didn't call them ,from Officer Lynch !!

March 25 at 7:39pm · Like



Sarah M. Landry Thanks for sharing! My husband has received multiple calls (which he never answered).

March 25 at 8:52pm · Like