AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 114–866

CATCH ME IF YOU CAN: THE IRS IMPERSONATION SCAM AND THE GOVERNMENT'S RESPONSE

HEARING

BEFORE THE

SPECIAL COMMITTEE ON AGING

UNITED STATES SENATE

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

WASHINGTON, DC

APRIL 15, 2015

Serial No. 114–04

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
49–469 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

Page

Opening Statement of Senator Susan M. Collins, Chairman 1
Opening Statement of Senator Claire McCaskill, Ranking Member 3

PANEL OF WITNESSES

PANEL I

Al Cadenhead, Ph.D., Senior Pastor, Providence Baptist Church 5
Jason Moore, Detective, Auburn Police Department 7

PANEL II

Julie Brill, Commissioner, Federal Trade Commission 22
Alysa D. Erichs, Special Agent in Charge, Homeland Security Investigations Miami, U.S. Immigration and Customs Enforcement, U.S. Department of Homeland Security 24

APPENDIX

PREPARED WITNESS STATEMENTS

Al Cadenhead, Ph.D., Senior Pastor, Providence Baptist Church 37
Jason Moore, Detective, Auburn Police Department 40
Julie Brill, Commissioner, Federal Trade Commission 47
Alysa D. Erichs, Special Agent in Charge, Homeland Security Investigations Miami, U.S. Immigration and Customs Enforcement, U.S. Department of Homeland Security 58

STATEMENTS FOR THE RECORD

Jason Moore, Detective, Auburn Police Department, Exhibit 1 69
Jason Moore, Detective, Auburn Police Department, Exhibit 2 71

CATCH ME IF YOU CAN: THE IRS IMPERSONATION SCAM AND THE GOVERNMENT'S RESPONSE

WEDNESDAY, APRIL 15, 2015

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

The Committee met, pursuant to notice, at 1:34 p.m., Room 562, Dirksen Senate Office Building, Hon. Susan M. Collins, Chairman of the Committee, presiding.

Present: Senators Collins, Heller, Cotton, Perdue, Tillis, Sasse, McCaskill, Gillibrand, Donnelly, and Kaine.

OPENING STATEMENT OF SENATOR SUSAN M. COLLINS, CHAIRMAN

The CHAIRMAN. The Committee will come to order. Good afternoon.

Today, our Committee continues its fight against the fraudsters, swindlers, and con artists that plague America's seniors. Our hearing this afternoon will focus on the IRS impersonation scam. We will examine how the scam works, what seniors can do to keep from falling victim to it, and what law enforcement is doing or is not doing to stop it.

The Treasury Inspector General for Tax Administration has called this scam the largest, most pervasive impersonation scam in the history of the IRS. According to the Inspector General, more than 434,000 Americans have been targeted by scammers impersonating IRS officials. Thousands of citizens have been defrauded of millions of dollars. The IG estimates that 10,000 IRS impersonation scam calls are placed each week.

As we will hear from our witnesses in greater detail in a few minutes, the scam often starts with a call like the one I am about to play, which was provided to us by the police department in Auburn, Maine, so if we could listen to the call.

[An audio recording was played.]

A rather ironic ending there.

Victims are told that they owe back taxes and will be arrested or, in some cases, deported if they do not pay up immediately. They are then instructed to purchase prepaid debit cards at local retailers, to load those cards with cash, and to read the PIN numbers on the back of the cards to the fraudsters. Armed with these PIN numbers, the fraudsters then transfer the money to their accom-

plices and wipe the cards clean of value. Scammers are also known to use wire transfers to steal money from their victims.

These methods are typical of the other scams that our Committee has investigated, but the IRS impersonation scam artists have added a pernicious twist. They are pretending to be government officials working for the IRS, a Federal agency that, frankly, makes most Americans apprehensive. When they get their victims on the phone, they warn them not to hang up, and if the call is terminated, a different scammer impersonating a local law enforcement official calls back immediately and threatens the target with arrest.

As best we can tell, many of these calls originate in boiler rooms in India, but the scammers use Voice Over Internet Protocol technology to spoof the caller ID to make it appear that the calls are being placed by the IRS or even local law enforcement, so when the unsuspecting victims see the Internal Revenue Service or the local police department pop up on their caller ID, they are terrified and easily hustled into doing whatever the scammers demand.

We have an excellent panel of witnesses today. First, we will hear from one of the victims, Pastor Al Cadenhead, who was defrauded of some $16,000 in just seven-and-a-half hours, and Pastor, I want to tell you how much I appreciate your willingness to come forward and tell your story publicly. You are going to save a lot of other people from going through what you did.

I am also delighted to welcome Detective Jason Moore of the Auburn Police Department in Auburn, Maine. Detective Moore will describe a case he handled just two weeks ago involving a constituent of mine who was defrauded out of $23,000. Detective Moore and his colleagues took quick action to stop the transfer of the victim's funds to the scammers and they were able to recover $11,000, so I congratulate him and the Auburn Police Department for their effective work.

I also want to welcome on our second panel Alysa Erichs, the Special Agent in Charge of the Miami Field Office for Immigration and Customs Enforcement. Ms. Erichs' office helped to prosecute and convict two individuals involved in the IRS impersonation scam, and for this good work, they also deserve our thanks.

Finally on the second panel, I want to welcome FTC Commissioner Julie Brill. The FTC plays an important role in educating consumers about how to better protect themselves from these scam artists.

Before I close my remarks, I want to note publicly my disappointment that the Department of Justice declined the Committee's invitation to testify before us today. As I noted at the outset of my remarks, thousands of Americans have been victimized by IRS impersonation scammers and 10,000 new scam calls are being placed each week. Actually, the number of victims is greatly understated because we know from previous experience that it is just the tip of the iceberg, that many victims are too embarrassed to come forward or they still do not realize that they have been taken.

Yet, despite all of this harm, it appears that the Department of Justice has prosecuted just three IRS impersonation con artists in the entire country, two of which were done in the case we will hear about in the second panel, and these were not even the criminal masterminds running the scams. They were low-level operatives.

I simply do not understand the Department's apparent indifference, and its refusal to testify before this Committee is completely unacceptable. I am left to conclude that the Department does not want to be held accountable or answer questions about its poor record.

There seems to be a pattern of lax enforcement by the Department of Justice when it comes to pursuing the various scams targeting seniors. If the Department contends that it does not have the tools or the resources it needs to protect American citizens against these scams, it ought to be working with us to get those tools, not refusing to testify.

After all, there are really only two remedies to these kinds of scams. One is educating the consumer so that the consumer can avoid becoming a victim, and second is going after the con artists and putting them in prison. That is a tremendous deterrent to others who would try to rip off our seniors and other citizens.

I do want to thank those witnesses who are appearing before us today and I look forward to their testimony.

Senator McCaskill.

OPENING STATEMENT OF SENATOR CLAIRE MCCASKILL, RANKING MEMBER

Senator MCCASKILL. Thank you, Chairman Collins.

With many Americans focused on their taxes today, this is a great opportunity to call their attention to this scam that is sweeping the Nation. This impersonation scam does not discriminate. We have seen a wide range of people targeted, from the young to the old, and it does not matter where you work or where you live.

The Inspector General for the IRS has received threatening calls, so too, have many Members of Congress. It seems that virtually everyone you talk to these days has either gotten one of these calls or knows someone who has.

It is easy to fall for this. To many victims around the country, you should not be ashamed of what happened to you. All of us have a natural fear of the IRS. It is in our DNA as Americans. I appreciate the bravery of someone like our witness, Dr. Cadenhead, who is stepping forward in hopes others can learn from his painful experience. It is easy to see why he and thousands of others have fallen for this. The IRS is an agency that does strike fear into Americans' hearts, and many are scared of both the tax code and its complexity and the agency itself, so when they receive a threatening call from what appears to be a 202 area code, it is no wonder that many people believe what they are hearing.

I am going to say something to the American people that should warm their hearts. If you get a call out of the blue from the IRS, do not answer it. Let it go to voice mail. Pick up the phone and hang it up. The IRS has told us very clearly that they only use the telephone as a last resort after sending multiple notices via mail, their preferred method of communication.

Furthermore, the IRS is never going to dictate a method for you to pay what you owe, so if you, for some reason, find yourself on a phone call with someone purporting to be an IRS agent demanding you send money through a debit card or a credit card without

giving you an option on how you want to pay, that should be another red flag.

Frankly, you should not even engage these people. If you are concerned that your call could be legitimate, call our Committee's fraud hotline to check it out. Call your Member of Congress. Call the FTC. Call the Inspector General at the Treasury Department. Or, call the IRS and talk to the IRS about the call you have received.

The FTC tells us this is one of the few scams where consumer education can, in fact, make a real difference, that once people know the IRS is not going to be calling them, these fraudsters will end up moving on to something else because this will no longer be a worthwhile endeavor.

I certainly hope so, because right now, the agency has generally seen more and more IRS impostor scam complaints every month. We are almost halfway to the number of complaints we got in all of 2014 and we are only through the first quarter of 2015. Whether more people are complaining because they are aware this is a scam or whether more people are actually being targeted is unclear, but we know we need to do something about it.

The Better Business Bureau of Southwest Missouri estimates hundreds of people have been called there and are calling this scam an epidemic. In 2014, FTC reports receiving more calls from Missouri about impostor scams than all other types of fraud except for debt collection, and the stories they have collected are heartbreaking.

One woman lost $15,000 after a man claiming to be an IRS agent threatened to arrest her and threatened a lien on all of her assets and a threat to notify her employer. Another woman detailed an 8-hour ordeal during which she handed over more than $16,000 to these criminals.

I am eager to hear from the FTC and law enforcement today about what they are doing to go after the fraudsters and to alert the public, and I thank Chairman Collins for bringing this to the attention of the American people by holding this hearing.

Let me also say that I share the Chairman's disappointment about the Department of Justice not being here today. Let no one think there is a dime's worth of difference between the Chairman of this Committee and the Ranking Member about the refusal of agencies of this government to participate in oversight hearings. There is no good excuse to not participate in an oversight hearing.

I will just say this to any agency in the future who thinks it is a good idea to ignore an invitation to come to this Committee in front of this Chairman. I know her. This does not mean she will go away, and by the way, I have got her back. I will not go away, so let the word go out that it is a bad idea to avoid a hearing in the Aging Committee when we are trying to get at solutions for a problem that is painful, real, and impacting innocent Americans all over this country.

Thank you, Madam Chairman.

The CHAIRMAN. Thank you very much for such a strong statement.

I am delighted now to call on our first witness, who is a constituent of Senator Tillis, Dr. Al Cadenhead, who is the Senior Pas-

tor at the Providence Baptist Church in Charlotte, North Carolina. Thank you so much for being here.

Senator Tillis, if you have any words of welcome for your constituent, feel free.

Senator TILLIS. I just hope we have been taking care of you since you have been here a little bit earlier. Thank you for traveling up, and we really do appreciate you coming forward and sharing your story. I think it is critically important. We need more to do it.

The CHAIRMAN. Thank you.

STATEMENT OF AL CADENHEAD, PH.D., SENIOR PASTOR, PROVIDENCE BAPTIST CHURCH

Dr. CADENHEAD. Madam Chairman, I am going to stick pretty close to my prepared text. As a Baptist preacher, I am not known for brevity, so I will stick close to that and try to move as quickly as possible and then absolutely entertain any question that you might have.

On October 28, 2014, I received a voice mail on my cell phone from a woman who identified herself as an agent for the Internal Revenue Service. In this voice mail, she said that I was being charged with tax fraud for serious miscalculations on tax returns from 2008 to 2011 and that I should return the call immediately or have my attorney contact them. She further stated that they were contacting the local authorities.

Assuming that it was a legitimate message, I returned the call at approximately 8:30 a.m. The woman indicated that I was in serious trouble and the charge of tax fraud was due to my not responding to numerous attempts to contact me, that they had actually left a letter on my front door. She said they had a photo of an agent placing an envelope on my door with a letter requesting that I contact the IRS immediately. I asked if I might see the photo. She said, no, because it will be used in court against me.

She told me that I should not interrupt her for any reason and that I should be taking notes of the conversation. I indicated that I was driving and could not write. She told me to find a place to pull over. I pulled into the parking lot of a school on my way to my church office.

She proceeded to tell me that they were issuing a warrant for my arrest, that they were placing a lien on my house and freezing my accounts because I had failed to cooperate. She also said that they would be notifying the local media about the arrest. This prompted enormous anxiety for me because so much of my role depends on my public image, and also I planned to retire in six months then, which is now only two weeks away, and certainly did not want to embarrass my church.

When I said I would like to contact my accountant, she told me that that would not be a good idea because the miscalculations were so blatant that the court would likely take his license from him, and she told me not to interrupt her and began to describe the court costs that I could anticipate.

When I asked if I could then correct the miscalculation and pay the amount, she told me that it was $4,900, and I said, may I pay that? She said, let me refer you to my supervisor. She then for-

warded me to a many who identified himself as Steve Evans, gave a badge number.

He told me that if I broke connection with him, the warrant would be filed. The only way to pay the amount owed would be through a Government Approved Center and by use of Green Dot Visa cards. He indicated that Rite Aid was a place that handled the Visa cards and gave me instructions on where the closest one was. I indicated that I must get the money from the bank. He told me to keep the phone in my pocket and under no circumstance say anything about the IRS or why I needed the money. I should get the money, then go to the Rite Aid store and purchase five Green Dot cards, load each one with $500, then come back to the car and scratch off the cards and give him the numbers. He said he must check to see if the funds went through, and while he did that, he switched me to an assistant, and that I must acknowledge every thirty seconds that I was on the line with him.

After successfully transmitting the scratched off numbers, he told me to go to another Rite Aid store and purchase five more. I followed the same procedure the second time.

Realizing that he had a gullible victim, he then said that he wanted to notify me that there was a miscalculation, that I owed another $5,000, so I went to the bank a second time, borrowed the money, then I proceeded to the Rite Aid store according to his instructions, and if I broke connection for any reason, the warrant would be issued immediately.

Thinking that I had cleared the matter, he indicated that I still owed $6,000 from 2008, so I went to the bank a third time, borrowed $6,000. The lady at the bank asked me if everything was okay. I responded it was just personal business. I followed the exact same protocol, and by the time I paid the $6,000, it was 3:30 in the afternoon, over six hours into the conversation. I told him that I had a medical appointment and needed to honor it.

This Steve Evans told me that he had good news for me, that I should receive a refund of $8,900. He had to clear it with the Attorney General's office and then he would instruct me on the method of the refund. He would contact me before six p.m.

Realizing then that I had been scammed, I immediately talked with my attorney. He, too, knew that I had been scammed. However, in my attorney's presence, I called Steve Evans back to inquire of the refund. He said that he was still waiting on the documentation from the Attorney General's office, that they were closed for the day, and that he would call me by 8:30 the next morning.

When I did not hear from him the next morning, I called him at 9:00 a.m. He then proceeded to tell me the next morning that I needed to forward another $4,900 in order to get my $8,900 back. By then, I had made a phone call to the local FBI. They had directed me to the Treasury Department.

With the thought that maybe my line might be tapped, I answered the phone again when Steve Evans called me back. I kept him on the line with hopes that possibly somebody might be listening in. He again threatened me, even though I told him I knew he was scamming me. I hung up.

Within ten minutes, he called me back on another number. Thinking it might be an agency of the government, I answered the call. It was Steve Evans again, making his familiar threats.

In summary, I will easily confess the question can be raised as to how could anybody be so gullible. The short answer is that I was the perfect victim. I had never had any issues with the IRS and had no idea how they operate. I was well aware that many years ago, my father had a very difficult experience with the IRS. They were very harsh with him, never responded when they found out his calculations were correct, so for all I knew, the call of the impersonators was very believable.

I am also fortunate that I have not had to pay fines for major traffic violations and had no reason to assume that payments should not be made by way of Green Dot Visa cards. The scammers also talked a lot about notifying the media, and in my profession, that could be a nightmare, so I was the perfect victim.

I am sharing my experience for one reason only. It is with hopes that my involvement might assist in stopping this scam and prosecuting these criminals. There is no way to gauge the amount of hardship they have created for so many individuals. I get no pleasure out of sharing such an embarrassing experience. My only reward for being public with my shame is to communicate to as many people as possible that the IRS does not do business over the phone and that when calls are received, hang up. That is my reason for being here today.

Thank you.

The CHAIRMAN. Thank you very much for your extremely helpful testimony.

Detective Moore.

STATEMENT OF JASON MOORE, DETECTIVE, AUBURN POLICE DEPARTMENT

Mr. MOORE. Chairman Collins, Ranking Member McCaskill, and members of the Committee, thank you for the opportunity to testify today.

As you know, I am a police detective with the Auburn Police Department in Maine. I have been there for 17 years, and I recently handled a case involving a 50-year-old grandmother from Auburn who was scammed out of $23,000 by someone posing as an IRS agent. The victim is very embarrassed and has requested anonymity, and so I will refer to her as Mrs. A for the purpose of this testimony.

Mrs. A came into the Auburn Police Department to report that she may have been scammed. She explained that she received a message on her home answering machine that stated she was being sued by the IRS. 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 a badge number.

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 said that she owed $4,982. He told her that if that was not paid by 5:00 p.m. that day, she would be arrested and liens would be placed on her property. Mrs. A explained that she had her grandchildren

with her and would be unable to pay that day. Mr. Rogers said that was no reason and 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 mailed 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. She then went to a Walmart and purchased multiple MoneyGrams that were directly loaded to a prepaid card. She was told to buy them using a different sender name for each MoneyGram. She was then sent to the nearest Bank of America branch, which is about thirty minutes away from her, and was instructed to wire funds to a specific account.

There was a technical issue which prevented the wire transfer, so the scammer sent her back to Walmart to purchase more prepaid cards. At 6:00 p.m., Mr. Rogers told Mrs. A the IRS is closing for the day and the legal action will be put on hold until 9:00 a.m. the following day.

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, her phone lost connection. She then received a call from the Auburn Police Department—at least the number displayed that—and she spoke with a person who claimed to be Lieutenant Green, though there is no one employed there by that name. Lieutenant Green said if she continued to hang up that she would be arrested. She explained that these are unintentional drops and he said that he would fax Mr. Rogers. After ending that call, Mr. Rogers called back and she asked if the fax had gone through and he said it had.

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

Mr. Rogers called back Friday morning. He was now claiming Mrs. A owed another $7,432. He had her speak to two other people who were supposed to be with the IRS, one an account manager and one an attorney. They had her make another deposit at the Bank of America—they had her make that deposit at the Bank of America.

Afterwards, they told her that they needed another $900 for document fees. She began to cry and was told if she continued to cry, they would hang up and the process would start all over again.

She was then told they had discovered another $14,322 that was due. They said they would settle for $10,500 that day and she would receive 40 percent back in her tax refund in three weeks.

Mrs. A was next directed to obtain $6,300 in money orders from Western Union, which she purchased and then shipped to a Days Inn in South Carolina. She was again continually threatened throughout 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 all the receipts for the transactions. When I was meeting with her, she received a call on her phone. She said it was them. I assumed this meant the scammer, so I answered. I found myself speaking with a male with an Indian-sounding accent. He asked to speak to Mrs. A and I told him he could not. The male persisted in his request to speak with her, so I hung up.

Within seconds, her phone rang again. I could see it was the same caller and I again answered. It was the same male again asking to speak to Mrs. A. I told him that every time he called, he would be speaking with me. He continued to ask to speak with Mrs. A, even saying "please." I was firm and rude with him to the point that he hung up.

Since Mrs. A had 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 somebody, but I eventually made contact with a Ms. Chauntel James, who is a Senior Investigator with the Fraud Investigations Group. Ms. James later advised that the 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 for victims in California and New Jersey totaling $34,000 from that same account. Bank of America has agreed to refund Mrs. A her $12,432. From speaking to Ms. James, I understand that if Mrs. A had torn up receipts as she had been instructed to do by the scammers, she may not have been able to recover her money.

On behalf of Mrs. A, I filed a complaint online with the Treasury Inspector General for Tax Administration. She received a call the next day, and an agent has been assigned and is working on 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 myself received one the day I first began investigating this. I feel that there are other victims who have not reported these crimes as they have fallen victim and may be too embarrassed to report it, or may be unaware that they were even scammed.

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 orders and prepaid card purchases were unchallenged by the retailers. She has been given little hope of recovering the remaining $11,000.

Again, thank you for the opportunity to testify. I would be happy to respond to any questions.

The CHAIRMAN. Thank you very much for your testimony and your effective work.

Dr. Cadenhead, I was struck by the fact that it appears no one at the Rite Aid questioned your buying so many cards, and Detective Moore talked about that he was surprised that there was not more questioning by the wire transfer companies. This has been an issue that we have raised before in our hearings, that is there not

a responsibility on the retailers' part to just question, without invading the privacy of the individual, but just raise some questions. Would that have been helpful in your case, Pastor?

Dr. CADENHEAD. Senator, I think early on, it would have been helpful, when I am totally covered up with angst about this whole thing, and this is how many Green Dot Visa cards it took in the course of one day to transfer $16,000 to them. You can only purchase five, or you could at that time only purchase five, load each one with $500, so you might think that—and I had to go back to the second—after noon, you can go back to the same Rite Aid again and purchase more. For four hours, you cannot purchase any more, but after four hours, you could.

Even then, nobody said, "Is there a problem?" My bank did. The lady at the bank did ask me. She said, "Dr. Cadenhead, is there a problem?" I just said, no, it is personal business, but nobody in the Rite Aid store even questioned that maybe something was going on when I continually went in and bought five at $500 each over and over.

The CHAIRMAN. Detective, do you think that that would have helped with Mrs. A's case, if someone at the wire transfer business had said, "Gee, is the reason that you need this money, or is there something we could help you with? You seem distressed."

Mr. MOORE. Yes, I do, and I simply asked her, I said, did anybody challenge you at any of these locations? You are buying multiple—and, especially when she is buying the MoneyGrams. She is instructed to get them all from different names, so not just Mrs. A, but Mrs. B, Mrs. C, Mrs. D. I think that would be a huge red flag to the retailer, but she was unchallenged at any location, Western Union or MoneyGram.

The CHAIRMAN. That is an extraordinary detail that I did not know until just now, that she was using different names and yet going to the same retailer. I mean, talk about a red flag. How much bigger a red flag could you have?

Mr. MOORE. I agree.

The CHAIRMAN. That is extraordinary.

Another element that both cases seem to have in common is the use of technology to spoof the call so that it looked like it was a legitimate call from government. Doctor, we were talking before the hearing.

Dr. CADENHEAD. Correct.

The CHAIRMAN. Could you talk a little bit about that and what led you to believe that it was truly the IRS calling you.

Dr. CADENHEAD. Yes. It showed a Washington area code, and I even asked at one point, what was the address, and this Steve Evans gave me the actual address of the IRS office here in Washington, and I would ask questions of it.

One thing that I might add about the warning that maybe some retailer might give is that they are incredibly intimidating—not the retailer, but the phone call. They convince you that you need to have the phone in your pocket, do not say anything about the IRS. You are almost afraid they will ask you at that point about it because you do not know what to say. He is listening to the conversation in my pocket. Even if they had said something, I would have

been very leery, at that early point, anyway, of saying much other than, yes, I just need it for personal business.

The CHAIRMAN. Well, I am struck in hearing both cases how ruthless the con artists are, but also how sophisticated and clever they are. If this were an agency other than the IRS that they were pretending to be, it is doubtful that the level of anxiety that you would have would be quite so high. If this did not have the constant threats and phone calls and explicit instructions, and in your case, Pastor, even knowing where your local retail Rite Aid was——

Dr. CADENHEAD. He directed me to them. He directed me to every Rite Aid, told me how to get there.

The CHAIRMAN. That is extraordinary, that kind of level of knowledge, and clearly, they used the threat of embarrassment, also, with both of the cases that we have discussed. I wonder, we have a lot of members present, so I am going to go on to the next questions, but I do want to thank you both.

Just one final point, and that is for Detective Moore. How important was it that you acted so quickly on this case, because one of the complaints we have heard when people go to the FBI or try to contact the Federal Government is nothing happens quickly enough to get that money stopped.

Mr. MOORE. It was vital. If I had delayed at all, I would not have been able to recover any money. I was fortunate on that day that I was aware of the case that had come in over the weekend and that I was able to turn my full attention to it. Before I even had a chance to call Mrs. A, I was actually reading the report and I found out she had come in on her own, so her coming in helped tremendously, too, so I could get going faster.

I spent a considerable amount of time on the phone that day trying to get hold of the Bank of America, because I knew that was my only chance to recover some of her money. I got passed around a lot, passed around a lot, but eventually, I got through to somebody who could help, and when I was speaking to her, she let me go because she noticed that the wire transfer was actively going out. The criminals were taking it as we were speaking, so if I had delayed, they would not have been able to notice that. They would not have been able to stop it, and we would not have been able to recover any funds, and not just Mrs. A's, but those two other victims in California and New Jersey.

The CHAIRMAN. Thank you.

MCCASKILL. I wonder, do the victims in California and New Jersey know that you saved their money?

Mr. MOORE. I do not know.

Senator MCCASKILL. Congratulations on that.

Mr. MOORE. Thank you.

Senator MCCASKILL. Dr. Cadenhead, did the criminals know that you were a pastor?

Dr. CADENHEAD. I have no way of knowing exactly. They very quickly began talking about public image, that they were notifying the media, and they really played that card well, and I do not remember telling them——

Senator MCCASKILL. Yes. The interesting thing that has happened is that criminals have the ability now with the Internet to

go in and find ministers or find people that have a public profile that might be more likely to be very concerned about——

Dr. CADENHEAD. Yes.

Senator MCCASKILL [continuing]. something happening in the public media, and certainly they had done the homework to figure out—which is not hard, I mean, from anywhere in the world, you can figure out where the nearest CVS or Walgreens or Rite Aid is, just by the beauty of the Internet.

Tell me what happens after you figure out that it is a scam and these are criminals. Other than praying for their souls, which they need a lot, because I do believe there is a special place in a bad place for people who do this, tell me about where you went and what you did as it relates to law enforcement.

Dr. CADENHEAD. I was fortunate in that the afternoon, that afternoon, late, I was at church with my attorney, whose daughter works in a firm that she works next to a person who was a former Assistant U.S. Attorney. She was able to give me some instruction about where to go, but the next morning, I immediately contacted the local office of the FBI and they instructed me to go to the Department of Treasury, that there was a website set up, to enter the information on that website, so I immediately did that, filled out the report, and beyond that, I did not hear anything else from anybody that day.

Senator MCCASKILL. Did you eventually hear from anyone else?

Dr. CADENHEAD. No.

Senator MCCASKILL. You have never heard from Federal law enforcement at all?

Dr. CADENHEAD. No. I did—I am also a writer for the Charlotte Observer and was to do a column that very next Saturday, the first Saturday after this occurred, and I called the editor and told him what had happened, would it be okay if maybe I talked about it in my column, and he said he would like to do more than that, that he would really like to have the paper cover the story, so he sent an Observer reporter out and it appeared on the front page of the Charlotte Observer that next Sunday morning.

That got the attention of folks in Raleigh, and then I got a call from the Attorney General's office, from the Better Business Bureau, and they set up a press conference, so the press conference immediately got the word out and some things began to happen after that, but did I hear from the FBI? No, not that I recall.

Senator MCCASKILL. Detective, you, in fact, have local jurisdiction for a fraud that occurs to someone who lives in Maine.

Mr. MOORE. That is a point in contention that we always come across with the prosecutors. Where did the crime actually occur?

Senator MCCASKILL. Yes, and this is the kind of crime that every prosecutor wants to be someone else's jurisdiction——

Mr. MOORE. Yes.

Senator MCCASKILL [continuing]. because it is incredibly challenging to catch these people, because they are—nine times out of ten, maybe 99 out of 100—the people who are actually talking are not in this country.

Mr. MOORE. Correct.

Senator MCCASKILL. They are located in a different country, and that is why the Federal authorities are so important here.

I was fascinated by the fact that this was supposed to go to a, was it a hotel, Days Inn in the United States?

Mr. MOORE. A Days Inn in Greenwood, South Carolina. She addressed that package simply to "Andy."

Senator MCCASKILL. To Andy at Days Inn?

Mr. MOORE. Yes.

Senator MCCASKILL. Did you have an opportunity, or do you know if anyone in Federal law enforcement had an opportunity to contact Days Inn and find out who Andy was, because, clearly, that is somebody who is on our soil.

Mr. MOORE. To my knowledge, the Treasury agent is following up on that.

Senator MCCASKILL. Okay.

Mr. MOORE. We have not been able to talk directly, but he has told Mrs. A that he has agents from that area following up on that.

Senator MCCASKILL. Well, one of the things——

Mr. MOORE. Mrs. A herself called down there and talked to staff and they thought they knew who that person's last name may be.

Senator MCCASKILL. Okay, because that is a huge get——

Mr. MOORE. Yes.

Senator MCCASKILL [continuing]. because once you grab one, then you turn the screws and all of a sudden you are talking to other people who are setting up these people in other countries who are actually making the call, so I think it is really important for us to keep following up with Treasury and with FBI about how many people have they actually arrested. Are you aware of any actual arrests and prosecutions that have occurred with the IRS scam?

Mr. MOORE. I am unaware of any.

Senator MCCASKILL. Thank you.

The CHAIRMAN. Thank you.

Senator Tillis.

Senator TILLIS. Thank you, Madam Chairman.

The question I had relates—well, first off, I just want to echo what the Chair and the Ranking Member said, that it is unacceptable for DOJ not to be here, because a part of what we need to do is figure out strategies we can use for effective prosecution. Hopefully, they will see the benefit of coming and visiting from time to time.

My question really relates to something that is in the staff memo and it is the IRS numbers by State. You may not have seen this, but it is a stack ranking of the incidents and the dollar loss, and I am wondering if there are, to your knowledge—you may not be aware, it may be a question for the other panelists—if there is anything to learn from some States that have relatively high populations but, relatively speaking, lower incidents of this sort of scam, or scams in general. Could it be possible that the State legislatures or through other agencies they provide a higher level of awareness to make it less likely that it occurs? Are you familiar with any States that seem to be ahead of the game or leading the charge more?

Mr. MOORE. I am not aware of that, and Maine being a somewhat rural State, I think maybe the word does not get out as well,

and so maybe these other States are more well informed, as you indicated.

Senator TILLIS. Yes. I think you all had about eleven incidents. I was just looking at North Carolina. It is probably—well, it is the ninth most populous State, but it is 41, or, let me see, somewhere down in the—maybe 30th or 35th in incidents. I was just curious, because one thing we did in the legislature was a little bit more financial—I should say, public awareness in general, so I am just curious if there is something we can learn from that as a part of prevention.

I am wondering what we do—when we talk about the retailers—when I think about a Rite Aid, I think about an 18-to 20-something kid that sees somebody coming up with five of these cards and they are just running them through like they are the deodorant or whatever else they are buying there. What more could we do, or do you know of anything, any collaboration with the issuers of these cards to really step that up and make people think about are you being scammed at that point of retail? Is that a significant point of opportunity or choke point for us?

Mr. MOORE. I agree with what you are saying and I think it comes down to a training education for the retailers, because, as you said, it is usually a young populous that is manning these and selling them, so that they should be made aware that some of these red flags, like Mrs. A is buying for Mrs. B and Mrs. C and Mrs. D, and she is buying six of them, all from a different name.

I think, internally, the computer system should at least flag that. The scammers are aware of it. They know what dollar amounts not to break, so they have her get multiple ones at the same dollar amount.

Senator TILLIS. Detective Moore, I had a question that had more to do with law enforcement. With respect to training, when somebody picks up the phone and says that I may be scammed, do we have adequate training at the local level for people to take that seriously, and do we have any kind of tools that are in place or discussion of tools that could be put into place to make it more likely that we can track back these things, because the way that they are structuring it on the Internet makes it virtually impossible, unless you know it is a scam from the beginning and you can kind of take advantage of that, but are there any, in law enforcement circles, discussions of, boy, if we had these tools, we could at least get back and claw back of some of these?

Mr. MOORE. I am not aware of the discussions, but there is always room for improvement. You know, I get one of these cases. I am not always exactly sure of the jurisdiction, who is going to handle it in the end, so I just do whatever I can up front to identify where the crime is occurring, who the criminal may be, and if I can at least stop the transfer of money, do that, and then, from there, look out to the larger Federal law enforcement agencies who may have the jurisdiction.

Senator TILLIS. Okay. Madam Chairman, just a comment. I think it is remarkable that we could have an agency where you would think it would be likely that you would get that kind of call, so that tells me that the IRS needs to spend some time not making it likely that the average person gets a call, thinks they are talking from

a heavy-handed regulator that they should be afraid of, that they would go to this act. I could see how anybody could do it. I think about my mother and other family members who have been subjected to it, but my mother does not like the IRS, so she is the one that hangs up on them, but it is—I mean, we really need to think about the image we project in these agencies so that you are afraid of a government agency and that would lead you—that creates the pretext for the scam to occur, and I think that says something about what we need to do a better job of in terms of projecting our image and more of a customer service image than a bullying entity.

Dr. CADENHEAD. There is one other dynamic here. We have been told that the scammers will also sell our numbers to other people, and since that day in October, I have gotten numerous calls from other attempts at other things, so there is a whole industry out there selling numbers to other scammers. It is amazing.

Senator TILLIS. Thank you.

The CHAIRMAN. Thank you very much.

Senator Kaine.

Senator KAINE. Thank you, Madam Chairman, and thank you to both of you for your testimony. Dr. Cadenhead, I really appreciate you being willing to make an example—be an example, even—in a difficult circumstance that was obviously painful and costly to try to teach others that, hey, do not fall for this. That has been—it is very admirable that you have done that, and the local coverage and national news coverage, I am sure, has helped a lot of people out, so I really appreciate you doing that.

Dr. CADENHEAD. I hope so.

Senator KAINE. Detective Moore, I just was kind of curious, when you were with your Mrs. A and she was getting the phone call, not having been in the kind of criminal investigations—I was a lawyer, but only a civil lawyer—if you were able to trace calls like that, would they be blocked? Would there be no way for somebody who is taking that call, if they think, I think this is definitely a scam, now what can I do to keep this person on the line so I can try to track them down—but, would that be a dead end, probably?

Mr. MOORE. Yes. I have no means to trace that call as it was happening.

Senator KAINE. Mm-hmm.

Mr. MOORE. For most—a number of her calls were spoofed. Like, she received a call from, supposedly from my agency, which was a spoof——

Senator KAINE. Yes.

Mr. MOORE [continuing]. received calls from our local District Attorney's office, that was a spoof, and I assume the number that he called from that day when I spoke to him was just a VOIP number, a Voice Over Internet Protocol——

Senator KAINE. I missed the beginning of Dr. Cadenhead's testimony. You indicated that the material suggests a lot of these may be coming from India, that it was an Indian-sounding voice. Was that the same case for you, Dr. Cadenhead?

Dr. CADENHEAD. Yes. One of the flags for me, finally, earlier in the afternoon—middle afternoon when I became aware that it was a scam—was that when I would come back to the car, scratch off the numbers, give them to this Steve Evans, he would disappear

and would say to me, "I am transferring this call to one of my assistants. Please hold and let him know every thirty seconds that you are still on the line." Every thirty seconds, I had to say, "Still on the line. Still on the line."

This happened several times, but everybody they transferred me to had an Indian accent. They all had American names. It was Steve and Mike and Susie, but they all had Indian accents, and I began to think—and the background noise, it sounds like you are in a cubicle and a lot of other business going on. It sounds just like what you might imagine at a floor of IRS agents.

It began to dawn on me that after all this time, there is not somebody whose name is Bubba or some kind of Georgia or North Carolina name with a Carolina accent. They all had Indian accents with American names.

Senator KAINE. Mm-hmm.

Dr. CADENHEAD. That was really one of the flags for me.

Senator KAINE. I guess, that is all part of making it very difficult to enforce against someone. If this is all largely done overseas, that really puts a dead end up or puts blocks up to enforcement.

All right. No further questions, Madam Chair.

The CHAIRMAN. Thank you very much, Senator Kaine.

Senator Heller.

Senator HELLER. Madam Chairwoman, thank you, and to the Ranking Member, for holding this hearing, especially on tax day. I think that makes it a little appropriate. I want to thank our witnesses, also——

Dr. CADENHEAD. Thank you.

Senator HELLER [continuing]. for taking time and being here today and sharing your experiences and your stories.

Ranking Member McCaskill and myself are no strangers to marketplace scams. We served together, she as Chairwoman and I as Ranking Member, for the Subcommittee on the Commerce Committee dealing with consumer protection, so we have heard a lot of this and have worked together trying to get to the bottom of some of these things.

The chart that Senator Tillis had that talked about the different States, Nevada lost nearly $300,000 recently to IRS impersonations, and they said they had 58 cases. My concern is this. We have 58 cases. For every time yourself, Doctor, comes forward and shares what you have done and goes to the authorities, there are numerous people that do not. You know, the 58 cases in Nevada are probably multiples of those kind of numbers, and I fear—do not feel alone in this. This is pretty large scale.

Now, just within the last couple of months, both my father and my daughter were affected by similar situations, not specifically like yours, but fortunately, they stopped it before it got too far, but they are shopping.

I guess my question, Doctor, is do you think they were trolling or do you think they were looking for you specifically in your case?

Dr. CADENHEAD. I can only guess. It appears that—keep in mind, this was six months ago, almost six months ago now, and it appeared they were a bit more specific then, but as the word got out, it is just my hunch that more and more people were willing to hang

up and not follow through and it required them making more calls, maybe less scrutinized.

I have received, because of the press conferences and the CBS coverage and some other networks, I have received letters and e-mails from people all over the country, and for them, the trigger for them was the Green Dot Visa card. When the scammers started talking about Green Dot, then they remembered the article or the news broadcast, and for some reason, that woke them up to the fact that this was a scam.

I really think, now, they are just calling indiscriminately. It is just a ramped up number, trying to get their business back up.

The reason I ask that question is if I were looking through the phone book for someone that was awfully trusting, I would think a senior pastor may meet that qualification. Do you know of others that are in the same field as yourself that have had similar issues, problems, questions, phone calls, concerns?

Dr. CADENHEAD. After I came forward publicly and it was covered in the paper, there have been several local ministers who said to me they had gotten the same call since that article——

Senator HELLER. Yes.

Dr. CADENHEAD [continuing]. and knew to hang up.

Senator HELLER. I would anticipate that they would think you were pretty trusting individuals of your fellow human beings.

Dr. CADENHEAD. Public image is pretty important.

Senator HELLER. Yes, and that makes sense, also.

You know, I regulated the securities industry in Nevada for 12 years and did all the research, background checks for all the securities fraud that was occurring in the State at that time and some of the stories are horrifying, of individuals who have a retirement account, they are in their 60's, 70's, and even 80's, losing this kind of money to similar types of scams, and the most difficult part is the restitution portion of it. Detective Moore, you talked about it. What is your experience? What has been your experience in restitution, the ability to get somebody's money back in similar cases like the Doctor's?

Mr. MOORE. Pretty much nonexistent. This is the only case I can think of where I was able to recover money.

Senator HELLER. Okay. Give me some background, Detective. How many cases have you had that are similar to this? You have been doing this, what, since 2006?

Mr. MOORE. As a detective, yes.

Senator HELLER. Okay.

Mr. MOORE. At patrol level, they handle those same calls, and if they reach a level where they can no longer handle it, it gets passed on, or if it is a larger scale.

Senator HELLER. Can you give me some kind of an idea how many cases like this you have dealt with?

Mr. MOORE. Personally, I cannot come up with a hard and fast number.

Senator HELLER. That is fine. That is fine.

Mr. MOORE. Probably just a handful, but——

Senator HELLER. In your office. In your office, I assume there are multiple detectives.

Mr. MOORE. Yes, and I would say we probably get at least one a month.

Senator HELLER. One a month.

Mr. MOORE. Of varying, different scams.

Senator HELLER. Right. Right.

Mr. MOORE. I dealt with one not too long ago involving Green Dots where a restaurant was called and the caller, pretending to be Central Maine Power Company and saying, if you do not pay by five today, we are going to shut your power off, and they just happened to get hold of the owner's mother. She unknowingly got a Green Dot card and paid it out, and I had—the only thing I had to followup on was a phone number. That went nowhere.

Senator HELLER. Again, share your experience with restitution in most of these cases.

Mr. MOORE. Slim to none. Outside of this case we are talking about today, I have never gotten money back from a scammer.

Senator HELLER. Madam Chairman, no further questions.

The CHAIRMAN. Thank you very much.

Senator Gillibrand.

Senator GILLIBRAND. Thank you, Madam Chairwoman.

I am very grateful for both of your testimony here today. I have had roundtables all across New York State on this very issue where I have met with seniors about how they have been targeted. They have been targeted on the phone. They have been targeted on the Internet. They have been targeted through the mail, and the experiences are all similar in that they are pressured, they are confused, they are made to have to make decisions quickly without the benefit of children or advisors, and the reality is, is our seniors have a trillion dollars of assets and so they are just a very ripe target for criminals.

What I would like from you, Detective, what can law enforcement do and advocacy organizations do better to inform seniors of how to protect themselves? In some of the roundtables I had, it was the first time seniors actually had someone come in and tell them, these are the things to look out for. These are the things that we have known have already happened in this community, and they are very grateful to get phone numbers and someone to call to verify if something is true or not. What has your experience been in trying to advise seniors of how they may be targeted in the future?

Mr. MOORE. Well, it is important, as you say, to get the word out. Some people do not want to believe they are in a scam, and no matter how much you show them and tell them that the evidence is that they are in a scam, they do not want to believe it, but it is really important just to get the word out. We have taken to social media. I have posted on my personal social media page, and as I field calls from people who are getting these same voice mails at home, I tell them it is a scam. Tell everybody you know that it is a scam. If it is truly the IRS, hang up and call back to verify. They will not object. A scammer will adamantly object every time.

Senator GILLIBRAND. Do you have any thoughts about how victims are targeted? I know in some of the examples in New York State, the criminals knew the names of the person's children, and so they might call—or grandchildren—and might call their grand-

mother and say, oh, "I am in school. I am in a lot of trouble. Can you wire $2,000 immediately? If I do not get this money, I am going to—" and, of course, the grandmother responds immediately. Have you had a sense of how sophisticated some of these criminals have been in terms of researching their victims in advance?

Mr. MOORE. I have not personally dealt with any of that level of sophistication. I have heard of similar scams to that.

Senator GILLIBRAND. Mm-hmm.

Mr. MOORE. The one with Mrs. A here, I believe she was just a victim of trolling. I think they are just calling numbers and wait and see——

Senator GILLIBRAND. Try to get one.

Mr. MOORE [continuing]. who calls back.

Senator GILLIBRAND. Mm-hmm.

Mr. MOORE. I did not get the impression they had any prior knowledge of her name or demographics or anything. The voice mail she received was generic. It did not address her, anything about her family. It simply stated, "This is the IRS. You are being sued. Call us back."

Senator GILLIBRAND. Doctor, did you ever have any conversations or information from your church community, from your local community about how seniors had been targeted in your community? Had you ever had any notion that this could happen to you?

Dr. CADENHEAD. Well, I have had several who talked about the same kind of scenario you just mentioned——

Senator GILLIBRAND. Mm-hmm.

Dr. CADENHEAD [continuing]. where they were contacted by someone who knew their name and also knew their grandson's name——

Senator GILLIBRAND. Right.

Dr. CADENHEAD. This has happened three or four times with people in our congregation, that they were in trouble and that they needed them to——

Senator GILLIBRAND. Send money.

Dr. CADENHEAD [continuing]. send some money.

Senator GILLIBRAND. Yes.

Dr. CADENHEAD. In fact, it happened to my own father in Georgia——

Senator GILLIBRAND. Yes.

Dr. CADENHEAD [continuing]. same thing exactly.

Senator GILLIBRAND. When your congregation talked about it, was it a service that your church was providing, or did it just come up in social conversation?

Dr. CADENHEAD. Social conversations, and of course, after October, I became the target for everybody's latest information on any scam going on, so it became sort of a topic, a fairly public topic after that.

Senator GILLIBRAND. Do you think communities would receive outreach from either law enforcement or church communities or community centers to begin to have classes on how you could be targeted, things to be careful of, how to respond to a caller asking for your bank account number, you know, all the scenarios that happen every day? What do you think the most effective medium

would be, for you personally or for the people you know well, to get that information out to them in a friendly and approachable way?

Dr. CADENHEAD. Well, people get their news in different ways now. Younger generations really do not always read newspapers, but older generations do. I think any information that can be passed along——

Senator GILLIBRAND. The newspaper might be a good venue.

Dr. CADENHEAD. Absolutely, and television. Most everybody still watches television. I think any way that you can get the word out. The way we get our news is different depending on the generation.

Senator GILLIBRAND. Right. Detective, what is your experience in that? What would you recommend if we were to create an avenue or a grant program or something that people could apply for funding? What would you recommend for the victims that you have helped?

Mr. MOORE. Any way to get the information out is helpful. I am not sure how my victim could have been addressed in advance, maybe through—maybe banks could provide pamphlets, but any kind of information, newspaper, television, so that people know what to expect, what the signs are that this is a scam and should hang up and call law enforcement, the police, to verify.

Senator GILLIBRAND. Mm-hmm.

Dr. CADENHEAD. I might add, too, that in most cities, the Better Business Bureau is ready to provide that kind of help. In Charlotte, they have an entire clinic they can perform for you, and a local congregation would be a great place for that to occur.

Senator GILLIBRAND. Yes. Maybe we could work through that, Madam Chairwoman, and find ways to get information out.

The CHAIRMAN. Thank you.

Senator GILLIBRAND. Thank you.

The CHAIRMAN. Thank you.

Senator Perdue.

Senator PERDUE. Thank you. First of all, thank you both for being here——

Dr. CADENHEAD. Thank you.

Senator PERDUE [continuing]. and Detective, thank you for your specific effort here.

I just have a couple questions of the Detective. Dr. Cadenhead, I am from Georgia, but I have spent a lot of time in Auburn-Lewiston, so I appreciate what you are doing up there. They did not call me Bubba when I was a kid, though.

I have a generic question. This is going to be very difficult, but I want to get your personal feelings on it. I mean, we know this is a difficult crime to measure because a lot of people do not report it. In your community and your experience, do you have any feel for what percentage of these crimes go unreported?

Mr. MOORE. I could not estimate how many go unreported, but in dealing with my victim, Mrs. A, I get the impression if it was not for the substantial amount of money, she may not have reported herself. I mean, she is just so embarrassed and mortified by this, and I get the impression of people even losing a few hundred dollars or even a few thousand may not report it.

Senator PERDUE. Right.

Mr. MOORE. Some of them may not even know. They may think that is how the IRS works these days.

Senator PERDUE. Dr. Cadenhead, in your congregation, do you have a feel for that?

Dr. CADENHEAD. Well, I think—I can only guess. I have no way of verifying it, but my guess is there are as many out there who have not reported it as those who have. I know how difficult it was for me to become open and public about this, and the only reason my wife and I agreed was that it might be of some help to other folks, but it was a difficult decision to make because it is very embarrassing.

Senator PERDUE. Yes, sir.

Detective, you know, a lot of these calls come into the local authorities or maybe the State authorities or whatever. What kind of training would you see would be fruitful to help these first-line service people help a potential victim or an, indeed, victim?

Mr. MOORE. Something as simple as maybe a checklist on who can assist—what agency can assist us with this. Like, I have no means to trace a lot of this, so to know who I can reach out to, and I turned to the Internet myself and that is how I came across the number for Treasury to report this, and I filled out the form on behalf of Mrs. A and they were very responsive. They got back to her the next day, but oftentimes, I am not exactly sure which agency to turn to for assistance.

Senator PERDUE. Did you seek Federal or State help in any of those cases that you have dealt with?

Mr. MOORE. Yes, whenever I can.

Senator PERDUE. What kind of responses did you get?

Mr. MOORE. This one, in particular, was—I filled it out and I provided her information and they got back to her the very next day, which I was very impressed with.

Senator PERDUE. And that helped you in this case, obviously.

Mr. MOORE. Yes. In the past, I have called the FBI and gave them, you know, this is what is going on, it is widespread scam we are dealing with. They took the information and I never heard anything again, so I do not know what they did beyond that.

Senator PERDUE. You both are very knowledgeable about this, obviously, from personal experience and helping the victims, but is there any sense in your mind that there are networks perpetrating this, or are these individuals, or do you have any sense of that in your experiences?

Mr. MOORE. Based on the way they pass the calls around to multiple people, it has got to be at least a small network. I could not estimate how large. I mean, they could be separate cells working. I mean, it could be a separate cell that called Dr. Cadenhead as opposed to called my victim, or it could be just one big network.

Dr. CADENHEAD. Because of the number of calls being made and the wide area over which those calls are being received, it has to be a network. There is no way any small group can make it happen, and all the calls, whether it is Steve or her or him or whoever the person might be, they are so similar. I mean, they are working for a script and they have a response for every question that you might raise. They can answer it and tell you exactly why you should not do this or should do that. They constantly talk about

protocol. Do not break protocol, they will tell you, or else we will file the warrant.

Senator PERDUE. Detective, I saw in your story they try to keep them on the phone while they are going through this perpetration of fraud, is that right?

Mr. MOORE. Yes, and that is the same thing that happened to Dr. Cadenhead that happened to my victim. Stay on the phone. Do not hang up. You know, when my victim lost connection due to the poor cell service at Walmart, they assumed she was hanging up on them, and that is when they spoofed the police department's number and called her back and said, "You are going to be arrested if you hang up again."

Dr. CADENHEAD. Within the first thirty seconds—no, within the first three minutes, he told me, "If you have a charger for your phone, go ahead and plug it in because you are going to need it today."

Senator PERDUE. Really.

Dr. CADENHEAD. He said, "If your phone goes dead, we are filing the warrant."

Senator PERDUE. How long were you on the phone?

Dr. CADENHEAD. Six-and-a-half hours.

Senator PERDUE. One last question. What can we do at the Federal level in your mind, Detective, and if either of you have a thought, I would welcome it. I am about out of time, but what can we do in terms of helping the local—you are the front line officer. You are going to get the call more than anybody else. What can we do to help you?

Mr. MOORE. Just knowledge about who we can contact for assistance, what assistance is available, and what the best protocols for responding to these are.

Senator PERDUE. Do you have any suggestions?

Dr. CADENHEAD. I think there are going to always be scammers. It is always going to happen, but I think the more you can publicize this kind of thing to get the word out, educate people, I think that is the other half of it, and it is just as important.

Senator PERDUE. Thank you both. Thank you.

The CHAIRMAN. Thank you very much.

I want to thank both of our witnesses on this first panel. You have added enormously to our understanding of the problem by giving us both the consumer perspective and the local law enforcement perspective. Thank you so much for coming to the hearing today.

Dr. CADENHEAD. Thank you.

The CHAIRMAN. I am now going to call forth our second panel, Commissioner Brill and Special Agent Erichs.

Commissioner Brill, if you could proceed with your testimony, please.

STATEMENT OF JULIE BRILL, COMMISSIONER, FEDERAL TRADE COMMISSION

Ms. BRILL. Good afternoon, Chairman Collins, Ranking Member McCaskill, and other members of the Special Committee. I am Julie Brill, a Commissioner at the Federal Trade Commission. Thank you so much for inviting me to speak with you about the

serious problem of IRS impostor scams. I am pleased to have the opportunity to discuss with you some of the FTC's efforts to help consumers avoid these scams.

The powerful stories that the witnesses on the first panel shared with you describe the MO that IRS impostors and other government impostor scam artists have developed and employ widely. Many consumers would be terrified to receive the kind of call that Dr. Cadenhead or Mrs. A received, and unfortunately, this sense of terror only feeds into a scam that too often succeeds.

As we heard, an IRS impostor catches a consumer off-guard with an unexpected phone call. The impostor often knows personal details, such as the consumer's name, her address and Social Security number, which convinces her that the call is real. The impostor tells a plausible story about how the consumer owes thousands of dollars in back taxes. He then—the impostor then threatens the consumer with a combination of dire consequences: Arrest, prosecution, deportation, or revocation of the driver's license that might be key to her independence. Then, the final hook. The consumer can avoid all of these problems with a simple but painful solution: Send money through a wire transfer or preloaded debit card immediately.

Consumers who are targeted by these scams might believe that they are not behind in paying their taxes, but they might also think that maybe they made a mistake and that they will be better off paying the amount of overdue taxes in order to make these problems go away. Dr. Cadenhead described vividly how impostors put these elements together, and I thank him, just as you all did, I thank him very much for coming forward to shed light on how these scams work so convincingly.

Dr. Cadenhead's experience is far from unique. This pernicious scam is growing rapidly. In 2013, the FTC received just over 2,000 complaints about IRS impostor scams. In 2014, the FTC received over 52,000 complaints about these scams. If the trends that we are seeing so far this year continue, we will reach nearly 90,000 IRS impostor scam complaints by the end of 2015.

While IRS impostors target many consumers, older Americans are particularly vulnerable to them. Seniors often share sensitive personal information, including their Social Security numbers, with a wide range of family members and service providers, including lawyers, accountants, financial advisors, and health care professionals. In many instances, seniors have accumulated assets that make them attractive targets to fraudsters, and some seniors may have diminished mental capacity and may not see the signs of fraud when it is in progress or once it is complete.

The FTC plays a leading role within the Federal Government in educating consumers about IRS impostor scams as well as assisting consumers who have fallen victim to one of these scams, and luckily, it is possible to educate consumers about how to avoid these scams, so consumer outreach is crucial.

As we say in our consumer education materials—and can you go to the first slide, please? Thank you so much. This is from our—this information, by the way, is on our website. We welcome any of you to link to it on your websites, but this is an informational poster that we have. What we tell consumers is that the IRS's first

contact with you will not be by phone or e-mail. The IRS will first contact you by mail only, and the IRS will not ask you to pay back taxes with a prepaid debit card or money transfer, just as we heard earlier today, so we tell consumers that if you receive a call or e-mail that appears to be from the IRS and they ask you to wire money or send a prepaid debit card, it is a scam.

We also provide tips to consumers who do receive these calls. Could we go to the next slide? Thank you. Do not give the caller any personal information. Write down the name and number of the caller. Hang up. Contact the IRS directly. Report the call by filing a complaint with the Treasury Inspector General for Tax Administration, as well as with the FTC. Warn family and friends.

IRS impostor scams are serious crimes and need to be prosecuted as such, just as you mentioned, Madam Chairman. As a civil law enforcement and consumer education agency, we at the FTC also think there is an important role here for consumer education, because we can teach consumers how to avoid these scams in the first instance.

I look forward to discussing these critical issues with you today and to continuing to work with you on them in the future. Thank you.

The CHAIRMAN. Thank you very much, Commissioner, for your testimony.

We are now going to pause for just a moment of silence in honor of the victims of the Boston Marathon bombings. The exact time is 2:49. We are very close to that time, and it seems appropriate for us to just pause for a moment of silence right now.

[A moment of silence was observed.]

Thank you. As one who has a friend whose son was severely hurt in that bombing, I thought it was important that we commemorate the day.

We will now hear from Special Agent Erichs. Please proceed.

STATEMENT OF ALYSA D. ERICHS, SPECIAL AGENT IN CHARGE, HOMELAND SECURITY INVESTIGATIONS MIAMI, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. ERICHS. Chairman Collins, Ranking Member McCaskill, and distinguished members, on behalf of Secretary Johnson and Director Saldana, thank you for the opportunity to discuss ICE's efforts to combat cross-border financial crimes, including consumer fraud scams.

Homeland Security Investigations, or HSI, is the investigative arm of ICE and conducts criminal investigations to protect the United States against terrorism and other criminal activity that threaten public safety and national security and to bring to justice those seeking to exploit our customs and immigration laws worldwide. In its investigative capacity, HSI enforces more than 400 Federal laws and regulations, with jurisdiction over investigations of crimes with a nexus to the U.S. border.

As you know, there are many fraud schemes, such as tax fraud schemes, bogus lottery and sweepstakes schemes, phony investment pitches, and business opportunities, and others which are growing increasingly sophisticated and international in scope. Per-

petrators will victimize consumers of all ages, backgrounds, and income levels, but the elderly are disproportionately targeted.

I understand the Committee is particularly interested in the scenario where the perpetrator impersonates an individual of legal authority over the phone, such as an IRS agent, attempting to collect a tax or a fee that the victim allegedly owes to the government. The scammer claims the tax or fee must be paid immediately or a warrant will be issued for the victim's arrest. Or, more urgently, the warrant has been issued and will be served following the call if the victim does not pay the amount requested immediately.

HSI investigates this and several other types of fraud schemes, as well. One of the most common types of telemarketing fraud is the lottery or sweepstakes scam. These schemes typically involve fraudulent telemarketers identifying themselves as a lawyer, customs official, or lottery company representative to a potential victim.

In a typical fraud scenario, potential victims are led to believe that they have won an international multi-million-dollar sweepstakes. The scammers tell the victims that in order to receive their winnings, they will need to pay an advance fee. The fee is usually described as a tax, insurance payment, or customs duty that must be paid to release the winnings. The victims are instructed to send the funds via mail, courier, wire transfer, or prepaid card. The winnings are invariably nonexistent and the scammers steal the victims' money.

Most of these scammers are articulate and can involve a variety of partners to defraud the victim over the course of a period of time, a strategy that serves to increase the complexity of the matter and leads to a greater credibility to the scheme itself. Scammers have also been known to repeatedly bombard their victims with nonstop calls, even employing verbal abuse, to coerce the victims to comply. Intimidated, confused, and exhausted, victims yield to the scammers' demands.

I would like to take a few minutes to walk the Committee members through this one particular type of scam. HSI, along with several of the law enforcement agencies, have been investigating a growing and pervasive scam where scammers, frequently operating overseas, will contact American victims, pretending to work for government agencies like the IRS and others, and they will falsely and fraudulently tell victims that they have a tax lien or have committed some crime and must pay a fine.

We have also seen scammers call individuals and claim to work for a local Attorney General's office. The scammer tells the victim that he or she will be charged with fraud, but that the victim could pay a sum of money to avoid being charged. Victims will agree to pay all or part of the money demanded, and then the scammers instruct them to purchase a third-party money transfer card and later provide scammers with the information from that card.

At that point, the scammers will have the information they need to collect the fraudulent proceeds. The money is then frequently transferred onto a loaded prepaid debit card which can be used to purchase money orders at a variety of reputable establishments. Those money orders can then be ultimately deposited into bank accounts that scammers control.

In one case, scammers stated that they purchased approximately $5,000 in money orders each day, six days a week. Over the course of nine months, our investigators estimated these scammers facilitated the transfer of $900,000 from victims to scammers operating overseas.

Outreach and education are critical components in addressing telemarketing fraud. For example, the HSI Cornerstone Outreach Program Initiative was launched in July 2003 and has grown into a robust, unparalleled financial outreach program. The success of the program is due in large part to the personalized collaboration with financial industry partners, sharing red flag indicators relating to consumer fraud activity. Bringing together the expertise from government and non-government is the core of the Cornerstone program in addressing financial vulnerabilities exploited by trans-national criminal organizations.

Thank you again for the opportunity to appear before you today. ICE looks forward to working with the Committee to reduce the potential for these criminals to harm our senior citizens.

I would be pleased to address any questions that you have at this time.

The CHAIRMAN. Thank you very much for your testimony.

I have to say that when we found out that only three people in the United States appeared to have been prosecuted for these IRS impostor schemes, that I did not expect that ICE, Immigration and Customs Enforcement at the Department of Homeland Security, would be involved. Could you explain the involvement of DHS in these cases? Are you only involved if there is an overseas nexus, or how do you get involved? I do not think the average consumer or victim would think that ICE would be a place to go to get help.

Ms. ERICHS. Thank you, Madam Chairman. Yes, ICE is in a unique position because, as I had mentioned in my testimony, we enforce over 400 Federal statutes. With that, we also have a significant presence internationally. We have 63 offices in 46 countries, and with our agency with the nexus to the U.S. border, we do investigate those crimes that have a nexus to the border.

In this case, it is money that is leaving the United States. It may be leaving the United States in the form of cash. It may be leaving the United States in the form of prepaid cards or wire transfers. We also have the authority to investigate money laundering investigations domestically under Title 18, which is shared authority with other agencies, as well.

We do feel that we are in a unique position to address this crime because of our overseas presence.

The CHAIRMAN. How did the case that you successfully prosecuted come to the attention of ICE? Walk us through what happened.

Ms. ERICHS. Yes, ma'am. The case came to us—it was actually referred to us from our U.S. Attorney's Office. The U.S. Attorney contacted us and told us of a victim who had indicated that he was contacted by somebody claiming to be from the U.S. Miami Attorney General's Office, obviously, sort of a blend of the U.S. Attorney's Office and the State Attorney's Office. That victim was told that he had to pay $750 or he was going to be charged with fraud.

The victim was able to at least say, I will make a good faith payment to hold it over while I look into the matter and agreed to pay $150. The victim was instructed to go purchase a prepaid care—a MoneyPak, excuse me—and load the MoneyPak with the money. Obviously, after that time, we were contacted and were able to get involved in the case, again, through the referral from the U.S. Attorney's Office.

In that particular instance, this victim was out of State. It was not within the Miami area of responsibility, but being able to determine through law enforcement efforts that the MoneyPak and the prepaid card associated with then loading of those funds was negotiated within the Miami AOR. We went to one of the stores where some of the transactions took place, had investigators go out and check it out and spoke with their loss prevention folks. Again, a lot of these, as indicated earlier, these are reputable businesses that are selling products that the general public does use, but are being, in this case, exploited by criminals.

We actually have an Organized Crime Retail Task Force within HSI Miami where we partner with the retailers in our area, and again, we do conduct outreach on a number of things, including boosters and theft, but also that these products, and the vulnerabilities that exist in the use of these products, or the misuse of these products.

They dealt with the local loss prevention person and that person was able to provide us with video. We subsequently were able to identify the folks, because, low and behold, the next day they came back and tried to negotiate another prepaid card, conducted a traffic stop, identified them, and from that point then used a variety of law enforcement methods to trace their habit, what they were doing, how they were moving the money and the cards, et cetera, until, ultimately, they were arrested and charged with the crime.

One interesting point of this is to show again, and I know it was mentioned earlier, how far they are willing to go. At one point during this case, in cooperation with Green Dot, we actually were able to receive information on the Green Dot cards very quickly which was able to assist us in this particular case, but we actually approached the targets and inquired whether or not they knew whose name the cards were held in and whether they were, in fact, that person, and whether they, in fact, knew that you are not supposed to negotiate a card that is not yours, and they put someone else on the phone to speak to us, posing as the cardholder, to try to convince us that this was a legitimate transaction that should be used.

What we are seeing in this case is very typical. It is a layering process. It is a layering process of taking someone's money initially and loading it into, either from a MoneyPak, which, thankfully, no longer exists through Green Dot, and then loading it onto prepaid cards, and then loading it onto another prepaid card, and then purchasing money orders. It is a layering process to further distance themselves from the victim, from attempting to find the trace—for law enforcement to trace to them.

The CHAIRMAN. Thank you.

Commissioner Brill, you mentioned the number of complaints that you have been receiving has soared, and I have a chart on complaints by month, consumer complaints. I am not sure if these

are all IRS impostor scams or whether it is scams in general, but for March of this year, just last month, it shows more than 8,000 complaints, which if you annualize it, it is 96,000 complaints.

What do you do when you get these individual complaints?

Ms. BRILL. Thank you. We run the National Consumer Data base, which is known as Consumer Sentinel, and all of these complaints are placed into our data base. Two-thousand law enforcement agencies at the Federal, State, and local level, as well as some of our international partners, have confidential access to this data base, and what we can do, we spot trends and that allows us to begin consumer education efforts, as we have done vigorously in this instance with respect to IRS impostor scams, but it also allows the local and State and other Federal criminal law enforcement agencies to figure out where the trends are and to proceed.

As you said yourself, Senator Collins, Chairman Collins, I believe, just as you believe, that there are two solutions to this problem, consumer education and putting them in jail. Those are the two solutions.

We do not have criminal authority, so our job is the consumer education side and the data base and the data trend side.

The CHAIRMAN. Thank you. I guess I would just say that I worry a little bit that consumers think when they file a complaint with you that that triggers a law enforcement response, and I have a feeling Senator McCaskill will get into this in more detail——

Senator MCCASKILL. I am going to.

The CHAIRMAN [continuing]. so I am going to yield to her.

Senator MCCASKILL. The two people that have been arrested in Florida, is that your case?

Ms. ERICHS. It is a case from my office.

Senator MCCASKILL. You are it. You have done it. You are the only one in the whole freaking country that has pulled this off?

Ms. ERICHS. We have very—we have numerous cases like this, but——

Senator MCCASKILL. Let me interrupt you, because here is what I am really frustrated about. We have got Treasury IG——

Ms. ERICHS. Mm-hmm.

Senator MCCASKILL [continuing]. got a website, file a complaint on a website. We have got the FTC. You can file a complaint and you do a data base. We have got the Department of Justice who is AWOL today. We have no idea what they are doing or if they care. We have ICE. I cannot figure out why ICE has jurisdiction here, criminal jurisdiction on these cases. It is surprising to me, too. We have Treasury, and then we have State and local prosecutors.

It appears to me that this is all this and no one is doing a comprehensive effort to get everybody in the room. I mean, if these people were moving crack cocaine or heroin, we would have inter-jurisdictional task forces immediately. I mean, inter-jurisdictional task forces are a bread and butter in law enforcement because people move across State lines. People move products internationally, and this is exactly what these cases are. These are networks of criminals that are working domestically. They are working internationally. They are moving money. It takes technical expertise.

The notion that it is not a local jurisdiction—sure, there is local jurisdiction. You can make local jurisdiction on these cases because part of the crime is committed locally. You can make Federal jurisdiction on these crimes, and obviously, somehow, we are finding jurisdiction in all these agencies.

Now, I am kind of yelling at you guys and you are not the ones to yell at, but who should I be yelling at that no one appears to be making this a priority? Thousands and thousands of people are being ripped off and we are good enough in America to catch these guys and we are not catching them, because I think, frankly, Special Agent, you have decided to do a good job on this and you just decided you were going to keep pulling that thread until you got a live one, but I do not think there are very many of you. You may be the only one that has actually cared enough to try to pull the thread and arrest people.

Can you guys explain to me why there is not someone that we can hold accountable for the fact that these people, this pastor who made a complaint, and all this money is disappearing and it does not appear that, writ large, law enforcement in this country cares much.

Ms. ERICHS. May I respond to this?

Senator MCCASKILL. Absolutely.

Ms. ERICHS. I just would like to be clear and go back if I—I do not think I said it earlier, that TIGTA did participate in the investigation with us, so they were very much involved in the success of that particular case that I had mentioned.

I would also like to clarify that that is just one type of scam. What we are looking at is they can call and represent themselves to be anything. Again, it could be an IRS agent. It could be a U.S. Attorney's Office official. It could be a Customs official. It could be a lottery sweepstakes winner. It is just the idea itself of that contacting folks by phone and telling them that they need to pay money to either collect their winnings or avoid being charged is the underlying principle here that we need to address, number one, especially mainly through outreach and education to stop the money from ever going.

What we do is we are in the business of trying to either stop that money at any point before it leaves the United States and gets into their hands, and there are multiple opportunities for us to do that, and again, we do have the unique authority to do that, but we do partner with many Federal, State, and local agencies in order to do that——

Senator MCCASKILL. Well, then why have we not arrested anybody?

Ms. ERICHS. We have actually had a significant number of arrests. We have initiated——

Senator MCCASKILL. On these IRS scams?

Ms. ERICHS. Well, that is what I am saying. It is a new—it is a newer scam, but——

Senator MCCASKILL. It is not. It has been around since 2013. That is like saying heroin is coming across the border and we are going to wait two years before we lock anybody up.

Ms. ERICHS. It is also—well, it is one that can develop from another ongoing scam, so they may say they are a lottery sweepstakes

winner, and then the next thing you know, the IRS is calling them to pay the taxes on their lottery winnings, so we see sometimes a development of these cases where they will go into it.

We have initiated a task force in Miami, in the Miami area, to make an operations link to telemarketing, but mainly we are doing this is because what we are seeing is that the organizations are overseas and the money is eventually going overseas. You do have domestic cells. You do have anywhere from your smaller group——

Senator MCCASKILL. Right.

Ms. ERICHS [continuing]. of operators to a larger group of operators, but our goal is to get the biggest fish possible, and again, in this case, we were fortunate enough that we were able to act on it. We also try to, even before we are notified of a crime, if we along with our partners at U.S. Postal Inspection Service do——

Senator MCCASKILL. I forgot Postal. Postal is in this, too.

Ms. ERICHS. Yes.

Senator MCCASKILL. That is another one.

Ms. ERICHS. If we do currency operations, we can try to detect outbound currency going to Jamaica by flight, by cruise ship, through the mail, express mail——

Senator MCCASKILL. How many task forces like the one in Miami exist in the country?

Ms. ERICHS. I would have to get back to you with an exact number from each office.

Senator MCCASKILL. I would like to know that. I would like to know how many inter-jurisdictional task forces there are on these scams, and this is the number one scam for IRS in the country and——

The CHAIRMAN. In its history.

Senator MCCASKILL. In its history, and this is a powerful scam, and there is a reason it is so effective, is people are scared to death of the IRS, so I want to know how many inter-jurisdictional task forces there are out there and why this is not gelling more quickly within the law enforcement community, and, unfortunately, you are really the only one in law enforcement that I can get my hands on right now, but believe me, I am going to keep trying, because this is really pretty outrageous that we do not have more of a clarion call within law enforcement to make this a priority.

Thank you, Madam Chairman.

The CHAIRMAN. Thank you very much.

Commissioner, did you want to add anything?

Ms. BRILL. I agree that this is a terrible scourge and I applaud your continuing effort in this area. We have seen impostor scams that are a little bit broader than just IRS. There are cases where the scam artists pretend to be from the Department of Justice, as you mentioned. We filed one case where a company—an entity claimed that they had an affiliation with the Federal Debt Commission—it does not exist—the Federal Mortgage Marketplace, Federal Enrollment Center, Federal Assistance Program, Federal Modification Assistance, and Federal Mortgage Counseling. We see a lot of this, particularly with respect to mortgage assistance and credit repair. It is a real problem.

The IRS impostor scams have this extra layer, as we have all been talking about, that really frightens consumers, and I just applaud your continuing efforts here.

The CHAIRMAN. What I want to make very clear, as I associate my comments with my colleague's, is that it is so frustrating for the average consumer, the average victim. Once they realize that they have been a victim, they do not know where to go. Thank goodness, my constituent went to her local police department, and thank goodness she ran into Detective Moore, who really cared enough to instantly go after it and was able to halt part of the wire transfer, but from what I heard from the Pastor today, he still has not heard back from anyone in Federal law enforcement who is going after anybody to try to get his money back.

I think that you cannot—most people have not heard of TIGTA. I mean, TIGTA, the Treasury Inspector General for Tax Administration—that does not come trippingly off the mouths of—out of the mouths of most of my constituents or constituents throughout America.

Senator MCCASKILL. Or Senators.

The CHAIRMAN. Most Senators, even, yes. In fact, I bet if we did a survey——

Senator MCCASKILL. Nobody would know what it is.

The CHAIRMAN [continuing]. nobody would know what it was, and would not know to go there, so I think the educational campaign needs to be broadened beyond prevention to say, what do you do if you think you are a victim.

I, too—I am so impressed that Special Agent in Charge Erichs went after these individuals, and I was amazed that ICE did that kind of thing, and I thought I knew a fair amount about ICE, but again, that is not who you would expect.

When we are talking about crimes that are originating in India, the Auburn Police Department, talented though it is, is not going to be able to pursue that kind of case, other than trying to halt the transfer in the first place.

I think we need a concerted effort by the Department of Justice, working with its partners in law enforcement across the Federal Government and at the State and local levels, and the FTC and the more educational agencies, to ensure that consumers know what to do, and the way we were able to really crack down on the Jamaica lottery scam was when, through pressure from this Committee, the Department of Justice finally started arresting people and extraditing people and making it clear to the Jamaican government that this was not going to be tolerated, and I, personally, was about to lead a boycott of tourists going to Jamaica until they changed their law, and they changed their laws.

We really need more of an effort in this area, and I hope that you will help us figure out what should be done.

Again, I want to thank my Ranking Member, Senator McCaskill, who you can tell was a whale of a prosecutor, for all of her insight and support and expertise, and thank you both for testifying today.

Ms. ERICHS. Thank you.

Ms. BRILL. Thank you.

The CHAIRMAN. I would like to thank all of our witnesses for testifying today. I hope that this hearing has helped to inform and

protect Americans from ruthless scams, but most notably the one that we have focused on today, the IRS impostor scheme. Each of you has provided us with a valuable perspective and we want to make sure that we do pursue what I see as the two remedies: Greater public education so that people can avoid becoming victims in the first place, but far, far more aggressive investigation and prosecution of these criminals who are ripping off blameless people and using the name of the Federal Government to do so. That is one reason that they are so successful.

Again, I want to express my extraordinary frustration and, indeed, anger at the Department of Justice for failing to cooperate with this Committee and to testify today. That is not something that we are going to tolerate, and I think you saw today that there will be unanimous outrage from this Committee if that lack of cooperation continues.

The Committee members and any members of the public will have until Friday, April 24th, to submit testimony, statements, or questions for the record.

Again, thank you all for being here today.

This hearing is now adjourned.

[Whereupon, at 3:12 p.m., the Committee was adjourned.]

APPENDIX

Prepared Witness Statements

Testimony Of Dr. Al Cadenhead
Hearing On The IRS Scam

Special Committee On Aging
United States Senate
April 15, 2015

On October 28 , 2014 I received a voice mail on my cell phone from a woman who identified herself as an agent for the Internal Revenue Service. In the voicemail she said that I was being charged with tax fraud for serious miscalculations on tax returns from 2008 to 2011 and that I should return the call immediately or have my attorney contact them. She further stated that they were contacting the local authorities. Assuming it was a legitimate message, I returned the call at approximately 8:30 AM.

The woman indicated that I was in serious trouble and the charge of tax fraud was due to my not responding to numerous attempts to contact me, and that they had actually left a letter on the front door of my house. She said they had a photo of an agent placing an envelope on my door with the letter requesting that I contact the IRS immediately. I asked if I might see the photo. She said no, because it would be used in court against. She told me that I should not interrupt her for any reason and that I should be taking notes of the conversation. I indicated that I was driving and could not write. She told me to find a place to pull over. I pulled into the parking lot of a school on my way to my church office.

She proceeded to tell me that they were issuing a warrant for my arrest, that they were placing a lien on my house and freezing my accounts because I had failed to cooperate. She also said they would be notifying the local media about the arrest. This prompted enormous anxiety for me because so much of my role depends on public image, and also I plan to retire in six months and I certainly did not want to embarrass my church. When I said I would like to contact my accountant, she told me that would not be a good idea because the miscalculations were so blatant that the court would likely take his license from him. She told me again not to interrupt her and began to describe the court cost that I could anticipate. I don't remember the exact amount but it was in excess of seventy thousand dollars. When I asked the amount of my miscalculations, she indicated that it was $4,900. Still believing this to be legitimate, I asked how I might pay the amount of the miscalculation. She said that in order for payment to be made, she would have to refer the matter to her supervisory.

She then forwarded me to a man who identified himself as Steve Evans and gave a badge number. He told me that if I broke connection with him, the warrant would be filed. The only

way to pay the amount owed would be through a Government Approved Center and by use of Green Dot Visa Cards. He indicated that Rite Aid was a place that handled the Visa Cards, and gave me instructions on where the closest on was. I indicated that I must get the money from the bank. He told me to keep the phone in my pocket and under no circumstances say anything about the IRS or why I needed the money. I should get the money and then go to the Rite Aid Store and purchase five Green Dot Cards and load each one with $500. Then, come back to the car and scratch off the cards and give him the numbers. He said he must check to see if the funds went through and while he did that, he switched me to an assistant, and that I must acknowledge every 30 seconds that I was still on the line. He told me that if I hung up, the warrant would be issued.

After successfully transmitting the scratched off numbers, he told me to go to another Rite Aid and purchase five more with the same instructions. He told me where the next closest Rite Aid would be. I followed the same procedure for the second time. Realizing that he had a gullible victim, he said they had just notified him that there were other discrepancies and that I owed another $5,000. He instructed me to follow the same protocol again. He repeatedly told me that I must follow protocol or face serious consequences. We went through the same procedure for the additional $5,000. So, I went to the bank a second time and borrowed the money. Then I proceeded to the Rite Aid stores according to his instructions. And, if broke connections for any reason, the warrant would be issued immediately.

Thinking I had cleared the matter, he indicated that I still owed $6,000 from the year 2008. So, I went to the bank a third time and borrowed $6,000. The lady at the bank asked if everything was ok. I responded that it was just personal business. I followed the exact same protocol and by the time I paid the $6,000, it was 3:30 in the afternoon, over six hours into the conversation. I told him that I had a medical appointment and needed to honor it. This Steve Evans told me that he had good news for me – that I should receive a refund of $8,900. He had to clear it with the Attorney General's Office and then he would instruct me on the method of the refund. He would contact me before 6:00 PM with the instructions.

Realizing then that I had been scammed, I immediately talked with my attorney. He, too, knew that I had been scammed. However, in my attorney's presence I contacted this Steve Evans to inquire of my refund. He said that he was still waiting on the documentation from the Attorney General's Office but they were closed for the day and that he would call me by 8:30 AM the next morning. When I did not hear from him the next morning, I called him at 9:00 AM. He then proceeded to tell me the next morning that I needed to forward an additional $4,900 to get the refund which now would be larger and that I needed to take care of this immediately or there would be serious consequences. When I told him I knew he was a fraud, he quickly told

me I would be very sorry for not following through with this. By then I had made a phone to the local office of the FBI and they had directed me to the Treasury Department. With the thought that maybe my line might be tapped, I answered the phone again when Steve Evans called me again. I kept him on the line with hopes that possibly the authorities might be listening. He again threatened me even when I told him I knew he was scamming me. I hung up. Within ten minutes, he called me back on another telephone number. Thinking it might be an agency of the government, I answered the call. It was Steve Evans again, making his familiar threats.

I am sharing my experience for one reason only. It is with hopes that my involvement might assist in stopping this scam and prosecuting these criminals. There is no way to gauge the amount of hardship they have created for so many individuals. I get no pleasure out of sharing such an embarrassing experience. My only reward for being public with my shame is to communicate to as many people as possible that the IRS does not do business over the phone; and, that when calls are received, hang up. That is my reason for being present with this body today.

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.

PREPARED STATEMENT OF JULIE BRILL

THE FEDERAL TRADE COMMISSION on

IRS Agent Impersonation Scam

Before the

SPECIAL COMMITTEE ON AGING UNITED

STATES SENATE Washington, D.C.

April 15, 2015

I. INTRODUCTION

Chairman Collins, Ranking Member McCaskill, and members of the Committee, I am Julie Brill, a Commissioner at the Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to present the Commission's testimony on Internal Revenue Service ("IRS") impersonation scams and identity theft. Protecting consumers against identity theft and its consequences is a critical component of the Commission's consumer protection mission.[2]

This testimony begins by describing the nature of identity theft generally and the Commission's nationwide complaint management and education and outreach efforts on identity theft. It then describes the Commission's work on IRS imposter scams and tax identity theft, including our recent efforts organizing Tax Identity Theft Awareness Week.

II. IDENTITY THEFT

Millions of consumers are victimized by identity thieves each year, collectively costing consumers and businesses billions of dollars and countless hours to repair the damage. As one example, the Bureau of Justice Statistics estimates that 16.6 million persons – or 7 percent of all U.S. residents ages 16 and older – were victims of identity theft in 2012.[3] Given the serious and widespread harm caused by identity theft, the Commission has devoted significant resources toward combating the problem. Since 2001, the Commission has used its civil enforcement authority to take action and obtain settlements in more than 50 cases against businesses that it

---

[1] This written statement presents the views of the Federal Trade Commission. My oral statements and responses to questions are my own and do not necessarily reflect the views of the Commission or of any other Commissioner.

[2] *See* Identity Theft and Assumption Deterrence Act, Pub. L. 105-318, 112 Stat. 3007 (1998). Criminal prosecutions under the Act are handled by the United States Department of Justice. The Act directs the FTC, a civil law enforcement agency, to establish the federal government's central repository for identity theft complaints and to provide victim assistance and consumer education. The repository of identity theft complaints, known as the "Identity Theft Clearinghouse," is discussed in greater detail below in Section IIA.

[3] *See* Bureau of Justice Statistics, *Victims of Identity Theft, 2012* (Dec. 2013), *available at* http://www.bjs.gov/content/pub/pdf/vit12.pdf.

charged with failing to provide reasonable and appropriate protections for consumers' personal information, or misrepresenting the protections they provide.[4] The FTC has also acted aggressively on two other key fronts – nationwide complaint management and consumer education and business guidance, discussed below.

A. Nationwide Complaint Management

The Commission collects, manages, and analyzes identity theft complaints in order to target its education efforts and assist criminal law enforcement authorities. The Commission manages the Identity Theft Clearinghouse, a secure online database of identity theft-related complaints. Identity theft victims can enter complaint information directly into the database via an online complaint form or by calling a toll-free identity theft hotline and speaking with a trained counselor. The Commission makes the Clearinghouse data available to over 2,000 American and Canadian federal, state, and local law enforcement agencies who have signed confidentiality and data security agreements.[5] Through the Clearinghouse, law enforcers can search identity theft complaints submitted by victims, law enforcement organizations, and the Identity Theft Assistance Center, a not-for-profit coalition of financial services companies. To assist law enforcement and policy makers, the FTC also routinely issues reports on the number and nature of identity theft complaints received by the FTC.[6]

---

[4] *See* Commission Statement Marking the FTC's 50th Data Security Settlement, Jan. 31, 2014, *available at* http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.

[5] For example, 48 Offices of the Attorney General have access to the Clearinghouse data.

[6] *See, e.g.*, FTC, *Consumer Sentinel Network Data Book for January - December, 2014* (Feb. 2015) (hereinafter "2014 Data Book"), *available at* https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2014/sentinel-cy2014-1.pdf. The 2014 Data Book shows that over 330,000 consumers reported some form of identity theft, which represents 13% of the total number of complaints submitted to the Commission. This makes identity theft the most frequently reported category of consumer complaints (excluding do-not-call complaints), continuing a pattern that started over a decade ago.

B. Consumer Education and Business Guidance

Consumer education and outreach is another important part of the Commission's mission. The Commission works to empower consumers by providing them with the knowledge and tools to protect themselves from identity theft and to deal with the consequences when it does occur. The Commission receives on average 37,000 consumer contacts each week through its toll-free hotline and dedicated website, of which approximately 6,300 are identity theft complaints. Both callers to our hotline and consumers filing complaints online receive information on steps they can take to prevent or recover from identity theft.

Further, the FTC makes available a wide variety of consumer educational materials, including many in Spanish,[7] to help consumers deter, detect, and defend against identity theft. For example, *Pass It On* is our newest education effort aimed at active older adults, people who are 65 and older.[8] The *Pass It On* program is designed to train seniors to educate others about consumer protection issues. *Pass It On* reinforces what older adults already know about some of the scams in circulation. It gives them the tools to start the conversation, and it asks them to pass the information on. The topics include: imposter scams, identity theft, charity fraud, health care scams, paying too much, and "you've won" scams.

The FTC also publishes a victim recovery guide *Taking Charge: What To Do if Your Identity is Stolen*[9] that explains the immediate steps identity theft victims should take to address the crime; how to obtain a free credit report and correct fraudulent information in credit reports; how to file a police report;[10] and how to protect their personal information. The Commission has

---

[7] Additionally, the FTC offers *Identity Theft: What to know, What to do*, in Chinese, Korean, Tagalog, and Vietnamese. *See* https://bulkorder.ftc.gov/publications/identity-theft-what-know-what-do.

[8] *See* www.ftc.gov/passiton and www.ftc.gov/pasalo.

[9] *Available at* http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf.

[10] The Fair Credit Reporting Act (FCRA) also provides identity theft victims with additional tools to

distributed more than 5.4 million copies of the recovery guide and has recorded more than 4.3 million visits to the Web version (both English and Spanish versions).

The Commission also sponsors OnGuard Online,[11] a website designed to educate consumers about computer security, including the importance of not disclosing personal information such as Social Security numbers ("SSNs") to possible fraudulent operators. OnGuard Online was developed in partnership with other government agencies and technology companies. Visitors to the site can download educational games and videos, learn more about specific topics, including phishing and social networking, and obtain useful tips and information in an interactive format. OnGuard Online and its Spanish-language counterpart, Alerta en Línea,[12] average more than 2.2 million unique visits per year.

The Commission also agreed to participate in an innovative program with the AARP Foundation in 2012. As part of the program, the FTC refers for individual peer counseling consumers over the age of 60 who have called the FTC's Consumer Response Center to complain that they have been victims of certain frauds, including lottery, prize promotion, and grandparent scams.[13] Last year, 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.[14]

---

recover from identity theft. For example, identity theft victims who provide police reports to a consumer reporting agency may obtain a seven-year fraud alert on their credit files, alerting potential users of their reports to exercise special vigilance in opening accounts in the consumers' names. In addition, victims may block fraudulent information on their credit files, obtain from creditors the underlying documentation associated with transactions that may have been fraudulent, and prohibit creditors from reporting fraudulent information to the consumer reporting agencies. *See* FCRA, 15 U.S.C. §§ 605A, 605B, 609(e), and 611.

[11] *See* http://www.onguardonline.gov.

[12] *See* http://www.alertaenlinea.gov.

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

[14] The consumers from whom the Foundation gathered data reported having lost more than $15 million.

The Commission directs its outreach to businesses as well, encouraging them to secure consumers' information so that it does not fall into the hands of identity thieves in the first place. The FTC widely disseminates a business guide on data security [15] and has developed both an online tutorial [16] and a blog post [17] based on the guide. These resources are designed to provide diverse businesses – and especially small businesses – with practical, concrete advice as they develop data security programs and plans for their companies. And, the Commission will soon provide more guidance for businesses as part of its *Start with Security* initiative, including hosting road shows and webinars as well as developing updated business guidance, to give companies practical advice about data security.

In addition, the FTC develops data security guidance for specific industries. For example, the FTC has developed specific guidance for mobile app developers as they create, release, and monitor their apps. [18] The FTC also creates business educational materials on specific topics – such as the risks associated with peer-to-peer ("P2P") file-sharing programs and companies' obligations to protect consumer and employee information from these risks. [19] Further, the FTC recently released guidance about ways to provide data security for Internet of Things devices, which includes tips such as designing products with authentication in mind and

---

[15] *See Protecting Personal Information: A Guide for Business*, *available at* http://www.ftc.gov/tips-advice/business-center/protecting-personal-information-guide-business.

[16] *See Protecting Personal Information: A Guide for Business (Interactive Tutorial)*, *available at* http://www.ftc.gov/news-events/audio-video/video/protecting-personal-information-guide-business-promotional-video.

[17] FTC Blog, *Time 2 Txt About Data Security Basics?*, Jan. 23, 2015, http://www.ftc.gov/news-events/blogs/business-blog/2015/01/time-2-txt-about-data-security-basics.

[18] *Mobile App Developers: Start with Security* (Feb. 2013), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/mobile-app-developers-start-security.

[19] *See Peer-to-Peer File Sharing: A Guide for Business* (Jan. 2010), *available at* http://business.ftc.gov/documents/bus46-peer-peer-file-sharing-guide-business.

protecting the interfaces between devices connected to the Internet.[20]

Further, the Commission leverages its resources by providing educational and training materials to "identity theft first responders" – the state and local law enforcement agencies who often are the first resources for victims.[21] The Commission also distributes a law enforcement resource CD ROM that includes information about how to assist victims, how to partner with other law enforcement agencies, how to work with businesses, and how to access the Identity Theft Clearinghouse. In addition, the FTC and its partners have provided in-person identity theft training to over 6,000 law enforcement officers from over 2,000 agencies.

The FTC also has encouraged the development of a nationwide network of pro bono clinics to assist low-income identity theft victims. As part of this initiative, the FTC has created a comprehensive guide for advocates providing legal assistance to identity theft victims. The Guide for Assisting Identity Theft Victims (*Pro Bono Guide*)[22] describes how advocates can intervene with creditors, credit reporting agencies, debt collectors, and others, and it provides self-help measures that victims can take to address their problems. Step-by-step instructions provide best practices for recovering from identity theft.

Finally, in response to the President's Executive Order of October 17, 2014 on Improving the Security of Consumer Financial Transactions,[23] the FTC is developing and implementing a plan to make the recovery process for identity theft victims quicker and less burdensome. In the coming weeks, the FTC will unveil a new IdentityTheft.gov to provide streamlined information

---

[20] *See Careful Connections: Building Security in the Internet of Things* (Jan. 2015), *available at* http://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf.

[21] Resources for law enforcement are available at www.ftc.gov/idtheft.

[22] The *Pro Bono Guide* is available at http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

[23] Exec. Order No. 13681, 79 Fed. Reg. 63,489 (Oct. 17, 2014).

for identity theft victims and people whose information is stolen. In later phases, the Commission will enhance the online victim assistance process to help people take steps online to recover from identity theft more easily.

III. IRS IMPERSONATION SCHEMES AND TAX IDENTITY THEFT

The Commission has seen a drastic increase in two types of tax-related scams. The first are government imposter scams, in which scammers impersonate government officials and contact consumers, often seeking personal information or claiming that the consumers owe money. Whereas the Commission received only 65,000 government imposter scam complaints in 2013, that number increased to over 159,000 in 2014.[24]

In particular, the FTC has seen a rise in IRS impostor scams, where scammers pretending to be IRS officials contact consumers, claiming they owe taxes. The FTC received over 52,000 IRS imposter scam complaints in 2014, and almost 22,000 during the first three months of 2015 alone. These fraudsters go to great lengths to deceive consumers, taking steps such as threatening arrest or deportation for failing to pay, demanding immediate payment via wire transfers or pre-paid debit cards, and sending bogus emails to further their scheme.

Of course, government imposter scams are not limited to the IRS; they affect all agencies – including the FTC. For example, the Commission recently filed a complaint alleging that First Time Credit Solution, Corp. deceived consumers by claiming to be affiliated with or licensed by the Commission, and falsely promising that they could remove negative information from consumers' credit reports and improve consumers' credit scores.[25] The court in this matter

---

[24] *See* 2014 Data Book, *supra* n.6, at 82 Appendix B3.

[25] *FTC v. First Time Credit Solution, Corp. et al.*, Federal Trade Commission, Plaintiff, v. First Time Credit Solution, Corp., No. CV15-01921-DDP-PJW (C.D. Cal. filed Mar. 16, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/152-3114/first-time-credit-solution-corp-ftc-credit-solutions.

issued a temporary restraining order that temporarily ceased operations and froze defendants' assets, and litigation is ongoing.

The FTC has aggressively pursued the perpetrators of other government imposter scams as well. For example, in a recent case involving a telemarketing scheme targeting senior citizens, the defendants allegedly called consumers and misrepresented that they were working on behalf of Medicare, claiming that they needed to verify consumers' identities using personal information that included their bank account numbers.[26] The defendants allegedly assured consumers that the information would not be used to debit their bank accounts, and that there was no charge for the new Medicare card or information about Medicare benefits. However, within a few weeks, consumers learned hundreds of dollars had been debited from their bank accounts. At the Commission's request, a federal court halted this scheme, and the FTC is currently litigating to permanently end the operation and return victims' money.

The Commission has also seen development of a second type of identity-theft related scam – so-called tax identity theft – which has been an increasing source of the Commission's identity theft complaints.[27] Tax identity theft typically begins when a thief files a fraudulent tax return using another individual's Social Security number and receives a refund electronically. Consumers typically discover they have been a victim of tax identity theft when they go to file their own tax return, only to be informed by the IRS that a return has already been filed in their name.

While identity theft is an equal opportunity crime affecting all age groups, tax identity

---

[26] *See FTC v. Sun Bright Ventures LLC et al.*, No. 8:14-cv-02153-JDW-EAJ (M.D. Fla. Sept. 4, 2014) (temporary restraining order), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3217/gmy-llc.

[27] In 2014, tax- and wage-related fraud accounted for more than 32% of the identity theft complaints, making it the largest category of identity theft complaints by a substantial margin. *See* 2014 Data Book, *supra* n.6, at 12.

theft impacts older Americans in particular. First, older Americans often share their personal identifying information – including SSNs – with a wide range of family members and service providers, including lawyers, accountants, financial advisors, and health care professionals. At the same time, they often have a lifetime of accumulated assets that make them attractive targets to con artists and identity thieves. In addition, some older Americans facing health challenges, restricted mobility, or diminished mental capacity may be less likely to detect identity theft, failing to regularly check their mail, bank, credit card, and financial statements, or obtain and review credit reports.

To help address these challenges, the Commission has dedicated significant resources to educate consumers about IRS imposter scams and tax identity theft. For the last two years, the Commission has hosted Tax Identity Theft Awareness Week to raise awareness about tax identity theft and provide consumers with tips on how to protect themselves, and what to do if they become victims.[28] This year, the FTC partnered with AARP and the Treasury Inspector General for Tax Administration (TIGTA) to focus on IRS imposter scams in particular, hosting webinars, town halls, and twitter chats.[29] Commission staff also developed blogs to provide data security guidance for tax preparers[30] and human resource professionals,[31] as well as consumer blogs about IRS imposter scams, resources such as infographics, and engagement with traditional

---

[28] *See* http://www.consumer.ftc.gov/features/feature-0029-tax-identity-theft-awareness-week.

[29] These efforts included hosting a national webinar with TIGTA with over 300 participants, a tele-town hall in Florida with the AARP with over 4,000 participants; and a Twitter chat that yielded over 6 million impressions.

[30] *See* FTC Blog, *Tax ID Theft Awareness: Tips for Tax Preparers Bear (P)repeating*, Jan. 15, 2015, http://www.ftc.gov/news-events/blogs/business-blog/2015/01/tax-id-theft-awareness-tips-tax-preparers-bear-prepeating.

[31] *See, e.g.*, FTC Blog, *HR Professionals: Deter Tax ID Theft with an Open-Door (but Closed-Drawer) Policy*, Jan. 27, 2015, http://www.ftc.gov/news-events/blogs/business-blog/2015/01/hr-professionals-deter-tax-id-theft-open-door-closed-drawer.

and social media.[32] Last year, the Commission partnered with the IRS and AARP to focus on the top ten states for tax identity theft, hosting events in each state.[33] Finally, the FTC has developed consumer guidance on both identifying and dealing with tax-related identity theft.[34]

The FTC has also focused specifically on the impacts of tax identity theft on older Americans. For example, in 2013 Commission staff held a forum to address identity theft affecting older Americans.[35] In addition to exploring medical and long-term care identity theft, the event also focused on tax and government benefits identity theft impacting older Americans. Panelists addressed issues including: (1) delivery of educational messages to older Americans; (2) selection of reputable tax preparers; (3) identity theft awareness among tax professionals; and (4) misuse of prepaid and reloadable debit cards. And, as part of its *Pass It On* campaign discussed above, the Commission has developed educational materials for older adults on identity theft and imposter scams.[36]

IV. CONCLUSION

The Commission will continue to play a central role in the battle against IRS imposter scams and identity theft, and looks forward to working with the Committee on this important issue.

---

[32] *See, e.g.*, FTC Blog, *My Very Own IRS Imposter Call*, Feb. 3, 2015, https://www.ftc.gov/news-events/blogs/external/my-very-own-irs-imposter-call-0; FTC Blog, *3 Ways to Use Tax Identity Theft Awareness Week to Help People in your Life*, Jan. 26, 2015, http://www.consumer.ftc.gov/blog/3-ways-use-tax-identity-theft-awareness-week-help-people-your-life; FTC, IRS Imposter Scams Infographic (Jan. 2015), *available at* http://www.consumer.ftc.gov/articles/0519-irs-imposter-scams-infographic.

[33] FTC Press Release, *FTC Announces National Tax Identity Theft Awareness Week, Jan. 13-17, 2014* (Nov. 25, 2013), *available at* https://www.ftc.gov/news-events/press-releases/2013/11/ftc-announces-national-tax-identity-theft-awareness-week-jan-13.

[34] *See* Tax-Related Identity Theft, *available at* http://www.consumer.ftc.gov/articles/0008-tax-related-identity-theft.

[35] *See* FTC Forum, *Senior Identity Theft: A Problem in this Day and Age* (May 7, 2013), *available at* www.ftc.gov/bcp/workshops/senior-identity-theft.

[36] *See supra* n.8.

U.S. Immigration and Customs Enforcement

STATEMENT

OF

ALYSA D. ERICHS
SPECIAL AGENT IN CHARGE
HOMELAND SECURITY INVESTIGATIONS MIAMI

U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT

REGARDING A HEARING ON

"CATCH ME IF YOU CAN: THE IRS IMPERSONATION SCAM AND WHAT IS BEING DONE ABOUT IT"

BEFORE THE

UNITED STATES SENATE
SPECIAL COMMITTEE ON AGING

WEDNESDAY, APRIL 15, 2015 – 1:30 PM
562 DIRKSEN SENATE OFFICE BUILDING

INTRODUCTION

Chairman Collins, Ranking Member McCaskill, and distinguished members of the Committee:

On behalf of Secretary Johnson and Director Saldaña, thank you for the opportunity to appear before you today to discuss the efforts of U.S. Immigration and Customs Enforcement (ICE) to combat cross-border financial crimes such as consumer fraud scams.

ICE has the most expansive investigative authority and the largest force of criminal investigators in the Department of Homeland Security (DHS). With more than 20,000 employees and a budget of nearly $6 billion, ICE has nearly 6,700 special agents assigned to more than 200 cities throughout the United States and 63 offices in 46 countries worldwide. Working with our other federal and international partners, ICE disrupts and dismantles transnational criminal networks by targeting the illicit pathways and organizations that engage in cross-border crime.

Homeland Security Investigations (HSI)

HSI is the investigative arm of ICE and conducts criminal investigations to protect the United States against terrorism and other criminal activity that threaten public safety and national security, and to bring to justice those seeking to exploit our customs and immigration laws worldwide. Notably, in fiscal year (FY) 2014, HSI investigations led to the disruption or dismantlement of 520 transnational criminal organizations. HSI made more than 32,000 criminal arrests and seized more than 2.3 million pounds of narcotics, 20,000 weapons, and $720 million in currency and monetary instruments.

In its investigative capacity, HSI enforces more than 400 federal laws and regulations, with jurisdiction over the investigation of crimes with a nexus to the U.S. border or functional border. To accomplish its mission, HSI focuses its broad investigative authority on three operational priorities – border security, public safety and counterterrorism/national security. HSI investigates customs and immigration crimes, including transnational criminal organizations (TCOs) engaged in illicit activity related to export enforcement, human rights violations, narcotics, weapons and contraband smuggling, financial crimes, cybercrimes and child exploitation, human smuggling and human trafficking, intellectual property theft and trade fraud, transnational gangs, and immigration document and benefit fraud.

Fraud Schemes

There are many fraud schemes such as tax fraud schemes, bogus lottery and sweepstake schemes, phony investment pitches and business opportunities, and others which are growing increasingly sophisticated and international in scope. According to the U.S. Federal Trade Commission in March 2013, consumers lose hundreds of millions of dollars annually to cross-border financial crimes such as telemarketing fraud. Sadly, in many cases the loss represents the victims' entire life savings.

Perpetrators will victimize consumers of all ages, backgrounds and income levels, but the elderly are disproportionately targeted. Perpetrators take advantage of the fact that elderly Americans may have cash reserves or other assets to spend on these deceptive offers. A survey conducted in 2013 by the American Association of Retired Persons found that 90 percent of respondents reported awareness of consumer fraud, yet two-thirds said it was hard to spot fraud when it is happening. The survey also shows that elderly victims find it difficult to terminate

telephone conversations, even when they say they are not interested in continuing a conversation. Also, the elderly may be reluctant to report the incident for fear of losing financial independence should their families discover the fraud. Scammers will even try to use a variety of schemes, especially when they find a potentially vulnerable victim including those who may suffer from a cognitive impairment.

I understand the Committee is particularly interested in the scenario where the perpetrator impersonates a person of legal authority, such as an Internal Revenue Service (IRS) Agent, attempting to collect a tax or a fee, that the victim allegedly owes the government. The scammer claims a tax or fee must be paid immediately over the phone or a warrant will be issued for the victim's arrest, or more urgently, the warrant has been issued and will be served following the call if the victim does not pay the amount requested immediately. However, HSI investigates several other types of fraud schemes as well.

One of the most common types of telemarketing fraud is the lottery or sweepstakes scam. These schemes typically involve fraudulent telemarketers identifying themselves as a lawyer, customs official, or lottery company representative to a potential victim. In a typical fraud scenario, potential victims are led to believe that they have won an international multimillion-dollar sweepstakes. The scammers tell the victims that in order to receive their winnings, the victim will need to pay an advance fee. This fee is usually described as a tax, insurance payment or customs duty that must be paid to release the winnings. The victims are instructed to send the funds via mail, courier, or wire transfer. The winnings are invariably non-existent and the scammers steal the victims' money.

Scammers will also try to impersonate a relative, as perpetrators can often find names of a vulnerable senior's loved one listed in an obituary. The impersonator will claim to be a loved

one, state that he/she has been arrested in Canada for driving under the influence and needs money to pay a fine to avoid being sent to jail. A similar scenario is a perpetrator impersonating a senior's relative claiming, while on travel, they were injured and had to be hospitalized so they need money immediately for the medical treatment until their insurance can be processed to cover their medical care.

As you can see from just this small sample of scenarios, the stories are quite varied but the results are the same. Scammers will utilize any scenario to convince the victim to transfer his or her money to the perpetrator over the phone.

Most of these scammers are articulate and can often involve a variety of partners to defraud the victim over the course of a period of time, a strategy that serves to increase the complexity of the matter and leads to greater credibility to the scheme. Scammers have also been known to repeatedly bombard their victims with non-stop calls, even employing verbal abuse to coerce victims to comply. Intimidated, confused and exhausted, victims yield to the scammer's demands.

Impersonating IRS and Government Officials

HSI, along with other law enforcement agencies, has been investigating a growing and pervasive scam where scammers, frequently operating overseas, will contact American victims. The scammers pretend to work for government agencies, like the IRS, and they will falsely and fraudulently tell victims that they have a tax lien, or have committed some crime and must pay a fine. HSI's primary focus is the underlying fraud and the related money laundering. In all instances, HSI seeks to ensure full investigative collaboration with the appropriate investigative

entities from the agency that is being impersonated. In cases where an IRS agent is being impersonated, HSI collaborates with the Treasury Inspector General for Tax Administration.

The scammers will then tell the victims to make a payment to the government agency using a third-party money transfer system. The scammers will work with partners in the U.S. to obtain and launder the fraudulent proceeds, before attempting to transfer them out of the country. Law enforcement estimates that this is a multi-million dollar scam.

For example, we have seen scammers call individuals and claim to work with a local "Attorney General's" office. The scammer tells the victim that he/she will be charged with fraud, but that the victim could pay some sum of money to avoid being charged. Victims will agree to pay all or part of the amount demanded, and then the scammers instruct them to purchase a third-party money transfer card, and later provide them with information on the card. At that point, the scammers will have all the information they need to collect the fraudulent proceeds. The scammers have even obliged requests for tracking or confirmation numbers, and provided addresses for real government offices.

The money is then frequently transferred onto a pre-paid debit card, which can be used to purchase money orders at a variety of reputable establishments. U.S.-based co-conspirators for the scammers purchase these pre-paid debit cards, load them up with fraudulent funds, and then purchase money orders at supermarkets and other locations. The money orders can then be deposited into bank accounts the scammers control. In one case, scammers stated they purchased approximately $5,000 in money orders each day, six days a week. Over the course of nine months, investigators estimated these scammers facilitated the transfer of $900,000 from victims to scammers operating overseas.

West African Transnational Criminal Organizations- Romance Scams

Over the past several years HSI investigators have also seen an increase in fraud scams against the elderly via West African Fraud syndicates, mainly through a scheme known as the Romance Scam. West African Fraud organizations strategically target recently widowed seniors due to their vulnerabilities and access to cash. The Romance Scams target the elderly via online dating sites, establishing a virtual relationship with them, and utilizing fictitious profiles. The organizations exploit the relationship by portraying an emergency and requests the victim "loan" them $5,000 to $10,000. If the victim attempts to discontinue their relationship with the organization, the scammer exploits the victim's embarrassment and attempts to employ them in conducting other fraudulent schemes, on behalf of the scammer, such as the cashing of fraudulent checks. If the victim contacts the scammer to tell him/her that they have been approached by law enforcement, the scammer in turn tells the victim that he/she is the police and they should continue working together.

Interagency Partnerships

In order to combat criminal organizations involved in romance scams, telemarketing, and government impersonation fraud schemes, HSI works closely with other DHS law enforcement components such as the U.S. Secret Service, U.S. Customs and Border Protection, the DHS Office of the Inspector General and the Office for Civil Rights and Civil Liberties, as well as with the Federal Bureau of Investigation, the U.S. Postal Inspection Service, the Treasury Inspector General for Tax Administration, and the IRS. In addition, because of the multi-jurisdictional and international challenges that these TCOs pose to U.S. law enforcement, operating in many U.S. states and in countries such as Canada, Nigeria, Australia and India, HSI and its partner agencies have teamed up with DOJ to produce a more coordinated enforcement

and prosecution effort. This effort involves law enforcement working jointly with prosecutors, our foreign law enforcement partners, and the financial industry. This, in turn, has led to a more collaborative law enforcement effort that will eventually lead to the disruption and dismantlement of these TCOs that are victimizing our senior citizens.

Cornerstone – Forging Partnerships with the Private Sector

The HSI Cornerstone Outreach Initiative was launched in July 2003 and has grown into a robust, unparalleled financial outreach program. The success of the program is due in large part to the personalized collaboration with financial industry partners.

HSI recognizes that our financial industry partners have critical and actionable information related to illicit financial activity and are the first line of defense against money laundering. ICE Special Agents also serve as subject matter experts in money laundering methods involving fraudulent schemes. Bringing together the expertise from government and non-government spaces is the core of the Cornerstone Program in addressing financial vulnerabilities exploited by TCOs.

HSI is actively engaging the financial industry's anti-money laundering executives to forge one-on-one partnerships, developing and sharing red flag indicators based on review of the financial flows relating to consumer fraud activity. These partnerships enable ICE to leverage the banking industry, money service businesses, and prepaid card issuers for intelligence and cooperation in investigating and prosecuting TCOs.

Payment Mechanisms

As the earlier example in my testimony demonstrates, the TCOs involved in these fraudulent schemes want to receive illicit proceeds quickly and anonymously. As I tried to show, one emerging method employed by scammers is to use money mules from the United States. Money mules serve as money consolidation points in the U.S., and eventually laundering illicit proceeds out of the U.S. to the source countries where the TCOs are based. The choice payment methods for the TCOs are money service businesses and prepaid cards. Money service businesses allow them to receive funds through structured payments made under reportable currency thresholds. Prepaid cards allow for the instantaneous transfer of funds. The funds can be loaded by a victim virtually on the internet or at a retail location. The prepaid card can also be mailed to the organization for use outside of the United States. Currently, U.S. law does not define prepaid cards as monetary instruments, limiting law enforcement's ability to investigate illicit prepaid cards encountered at any U.S. Border.

CONCLUSION

Thank you again for the opportunity to appear before you today to discuss our efforts to combat consumer fraud scams which target our seniors, particularly those schemes where perpetrators try to impersonate IRS or other government officials to attempt to collect a made-up tax or fee. We look forward to working with you to reduce the potential for these criminals to identify susceptible targets, move their illicit funds, and address the issue of the penalties for these crimes meeting the seriousness of the harm they inflict on our senior citizens.

I would be pleased to address any questions you have at this time.

Statements for the Record

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.

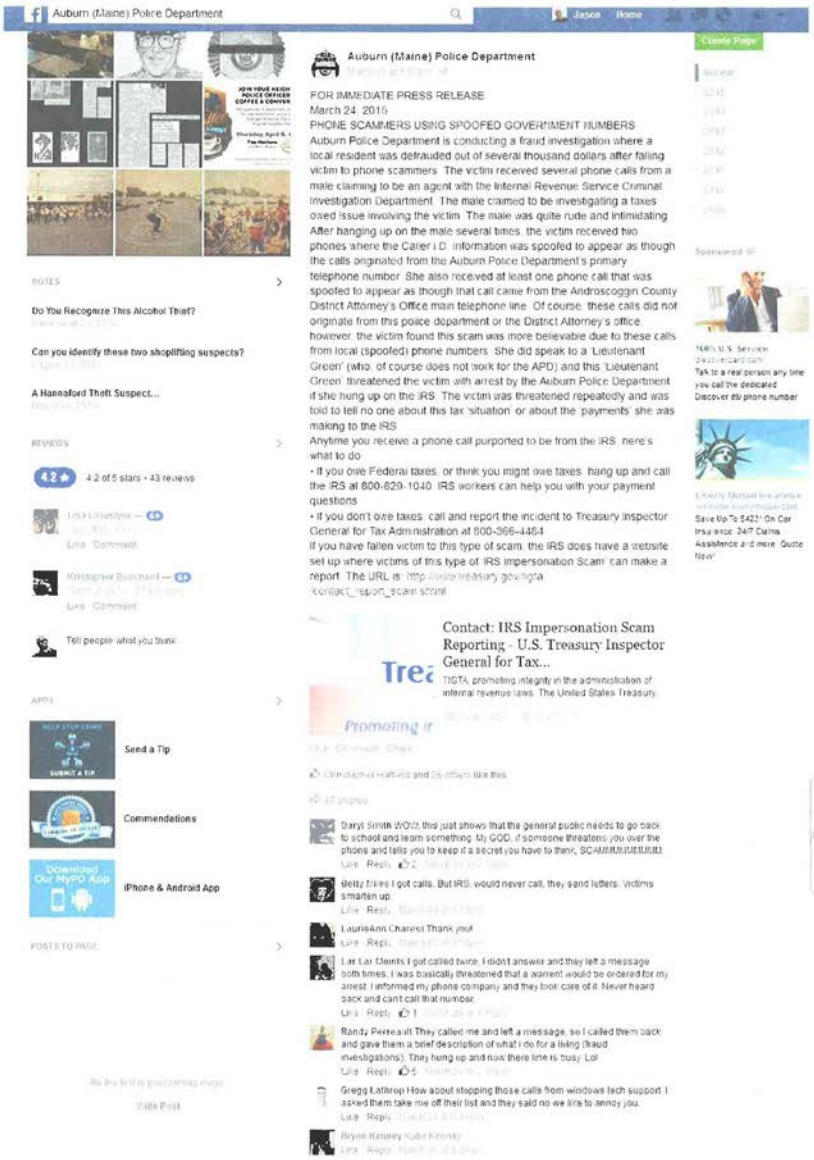
Anytime you receive a phone call purported to be from the IRS, here's what to do:

- 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
Jason Home
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 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
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
Promoting it
Do You Recognize This Alcohol Thief?
Can you identify these two shoplifting suspects?
A Hannaford Theft Suspect...
REVIEWS
4.2 of 5 stars • 43 reviews
Tell people what you think
APPS
Send a Tip
Commendations
iPhone & Android App
POSTS TO PAGE
Create Post
Create Page
Sponsored
Talk to a real person any time you call the dedicated Discover elo phone number
Save Up To $425* 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...

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 7:07pm · 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