AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

PREVENTING HARASSMENT THROUGH OUTBOUND NUMBER ENFORCEMENT (PHONE) ACT

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

ON

H.R. 5304

NOVEMBER 15, 2006

Serial No. 109–154

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://judiciary.house.gov

U.S. GOVERNMENT PRINTING OFFICE

30–839 PDF WASHINGTON : 2006

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

F. JAMES SENSENBRENNER, JR., Wisconsin, *Chairman*

HENRY J. HYDE, Illinois
HOWARD COBLE, North Carolina
LAMAR SMITH, Texas
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
DANIEL E. LUNGREN, California
WILLIAM L. JENKINS, Tennessee
CHRIS CANNON, Utah
SPENCER BACHUS, Alabama
BOB INGLIS, South Carolina
JOHN N. HOSTETTLER, Indiana
MARK GREEN, Wisconsin
RIC KELLER, Florida
DARRELL ISSA, California
JEFF FLAKE, Arizona
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TOM FEENEY, Florida
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas

JOHN CONYERS, JR., Michigan
HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California
LINDA T. SÁNCHEZ, California
CHRIS VAN HOLLEN, Maryland
DEBBIE WASSERMAN SCHULTZ, Florida

PHILIP G. KIKO, *General Counsel-Chief of Staff*
PERRY H. APELBAUM, *Minority Chief Counsel*

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

HOWARD COBLE, North Carolina, *Chairman*

DANIEL E. LUNGREN, California
MARK GREEN, Wisconsin
TOM FEENEY, Florida
STEVE CHABOT, Ohio
RIC KELLER, Florida
JEFF FLAKE, Arizona
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
LOUIE GOHMERT, Texas

ROBERT C. SCOTT, Virginia
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ANTHONY D. WEINER, New York

MICHAEL VOLKOV, *Chief Counsel*
DAVID BRINK, *Counsel*
CAROLINE LYNCH, *Counsel*
JASON CERVENAK, *Full Committee Counsel*
BOBBY VASSAR, *Minority Counsel*

CONTENTS

NOVEMBER 15, 2006

OPENING STATEMENT

	Page
The Honorable Howard Coble, a Representative in Congress from the State of North Carolina, and Chairman, Subcommittee on Crime, Terrorism, and Homeland Security	1
The Honorable Robert C. Scott, a Representative in Congress from the State of Virginia, and Ranking Member, Subcommittee on Crime, Terrorism, and Homeland Security	2

WITNESSES

The Honorable Tim Murphy, a Representative in Congress from the State of Pennsylvania	
Oral Testimony	5
Prepared Statement	7
Mr. Barry Sabin, Deputy Assistant Attorney General, Criminal Division, United States Department of Justice	
Oral Testimony	8
Prepared Statement	10
Mr. James Martin, President and Founder, 60 Plus Association	
Oral Testimony	18
Prepared Statement	19
Mr. Phil Kiko, General Counsel and Chief of Staff, Committee on the Judiciary, United States House of Representatives	
Oral Testimony	21
Prepared Statement	22

PREVENTING HARASSMENT THROUGH OUTBOUND NUMBER ENFORCEMENT (PHONE) ACT

WEDNESDAY, NOVEMBER 15, 2006

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CRIME, TERRORISM,
AND HOMELAND SECURITY
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 10:01 a.m., in Room 2141, Rayburn House Office Building, the Honorable Howard Coble (Chairman of the Subcommittee) presiding.

Mr. COBLE. Ladies and gentlemen, before I convene today's hearing, we have virtually no one except the Ranking Member and me here, but I want to say this before we start. This will likely be our final hearing on this Subcommittee, and I would be remiss if I did not express my thanks to each Member who served on this Subcommittee, and, in particular, the distinguished gentleman from Virginia, the Ranking Member, Mr. Scott; Mr. Vassar, his able counsel; Mr. Mike Volkov, and his able associates on our side. I think we have had a very productive 2-year stint during this session, and I'm appreciative to all of you on the Subcommittee. We have had good hearings. We've had good witnesses, today being no exception. And having said that, we will commence.

I want to welcome everyone to this important hearing regarding fraudulent telephone calls. Today the Subcommittee will be conducting a legislative hearing on the PHONE Act, H.R. 5304, the "Preventing Harassment through Outbound Number Enforcement Act," which was introduced by our colleague, Representative Timothy Murphy, who represents Pennsylvania's 18th Congressional District.

In the last few years, the criminal activity known as "spoofing" has increased. Those who engage in spoofing use an incorrect, fake, or fraudulent caller ID to conceal their identity in order to facilitate a fraudulent telephone call to the recipient.

Caller ID spoofing involves making one's own phone number and identifying information with another phone number and identifying information. Call recipients then divulge personal and private information to the caller under the mistaken belief that the caller is legitimate; that is, a bank, a credit card company, a court of law, et cetera. If the recipient of the call had known the true identity of the caller, the recipient would not have provided the private information.

Spoofing also invades the privacy of those individuals whose caller ID is used to mask fraudulent calls. Some may describe spoofing as a way to maintain caller privacy, but it is nonetheless fraudulent. Although the technology needed to spoof has been available for some time, it requires special equipment and knowledge to actually use the masking technology. Recently, this technology has become more accessible to the average person, either through the purchase of Internet telephone equipment or through Web sites specifically set up to spoof. These Web sites claim to be set up to protect your privacy. However, the use of this technology has been linked to fraud, prank telephone calls, political attacks, and telemarketers who attempt to avoid the current "do not call" limits. Additionally, calling cards can be purchased or accounts can be set up to allow multiple calls. Further, the technology can block any back technology such as the star symbol or dash 69.

Representative Murphy introduced H.R. 5304 to address these concerns by creating a new Federal crime to prohibit the modification of caller ID with the intent to deceive the recipient of a telephone call as to the identity of the caller. The bill imposes a fine and/or a prison term of up to 5 years for violations.

However, the legislation does not affect legally available blocking of caller ID technology or lawfully authorized activities of law enforcement or intelligence agencies. This legislation is intended to help protect consumers from harassment, identity theft or other crimes. This hearing will focus on the need to broaden the scope of current law to deter telephone fraud, protect consumers from harassment and to better protect consumers and their personally identifiable data from fraudulent telephone use, and also the need to increase the tools available to the Department of Justice to prosecute and protect against criminals who use fake telephone and caller ID to commit crime.

I look forward to learning more about this bill this morning, and thank each of our witnesses for participating in today's hearing. And before we call upon our witnesses, I am pleased to recognize the distinguished gentleman from Virginia, the Ranking Member, Mr. Bobby Scott.

Mr. SCOTT. Thank you, Mr. Chairman. And, Mr. Chairman, you indicated that this may well be the last hearing that we have this session and you would be Chairman, and I'd like to comment on our working relationship. In commenting on it, I'm reminded of what President Kennedy said when he began a speech in Cleveland, Ohio. He said that there's no city in the United States in which I've received a warmer welcome and fewer votes than Cleveland, Ohio.

I think there is no Committee in Congress where I have enjoyed a warmer reception and fewer votes from the Chairman, but you've been very cordial and you've given everyone an opportunity to be heard, and I wish you well in whatever Committee that you're on next in the next session.

Mr. COBLE. If the gentleman will yield, those roles may well be reversed in about a month, but it's been a pleasure, Bobby.

Mr. SCOTT. Thank you. But I'm pleased to join you in convening this hearing on the PHONE Act. This bill is aimed in preventing the practice called "spoofing," where a caller uses a fake or fraudu-

lent caller ID to hide his true identity in order to irritate, harass, or defraud the recipient of the call.

I'm concerned about the growing aspects of spoofing being used for such purposes with impunity, and support the thrust of H.R. 5304. However, I think we need to make sure that the bill appropriately defines what constitutes spoofing or caller ID deception to the extent that criminal penalties should apply and what the penalty should be for what kind of spoofing intent. We also need to consider whether or not the mere act of altering one's caller ID information should be criminalized in those situations where there is no indication of intent to harass, defraud, or otherwise commit a criminal act.

Certainly the kinds of problems we expect to hear about today from our witnesses, including our own chief counsel, are the kinds of situations where we do want them to be covered under the bill as criminal acts. However, when there is no intent to defraud or harass, we need to consider whether or not innocent disguises of one's identity should constitute a crime. Disguises are routinely used in Internet names such as wildchild@aol.com or mr.niceguy@yahoo.net, and we need to consider whether or not the bill should criminalize using a similar caller ID for innocent purposes.

So I'm looking forward to the testimony by witnesses, Mr. Chairman, and for guidance on insight on these issues and in working with you as we develop a bill to address the problems of spoofing that we definitely want to prevent.

Thank you Mr. Chairman.

Mr. COBLE. Thank you, Mr. Scott, and thank you for your generous words as well.

Gentlemen, it is the practice of this Subcommittee to swear in all witnesses. So, if you all would please raise your right hand and stand, if you will.

[Witnesses sworn.]

Mr. COBLE. Let the record show that each of the witnesses answered in the affirmative. Please be seated.

We are blessed with a very distinguished panel today, and for the benefit of those in the audience who may not know the identities of the witnesses, I want to give you some background about them.

Our first witness is the Honorable Tim Murphy who is the representative of Pennsylvania's 18th District and is the primary sponsor of the bill we're addressing today, H.R. 5304. Congressman Murphy is a Member of the Energy and Commerce Committee and has three Subcommittee assignments, including the Subcommittee on Commerce, Trade, and Consumer Protection. From 1997 to 2002, he served in the Pennsylvania State Senate where he penned the State's historic patient bill of rights and increased funding for medical research. Since his election to Congress in 2003, he has continued to be a leader in health issues as a member of the Congressional Mental Health Caucus and the 21st century Health Care Caucus. Congressman Murphy holds a bachelor's degree from Wheeling Jesuit University, a master's degree from Cleveland State University, and a Ph.D. from the University of Pittsburgh.

Our second witness is Mr. Barry Sabin, Deputy Assistant Attorney General of the Criminal Division of the United States Department of Justice. In this capacity, Mr. Sabin is responsible for overseeing the Fraud Section, Criminal Appellate Section, Gang Squad, and Capital Crimes Unit. Mr. Sabin served as the Chief of the Criminal Division's Counterterrorism Section from 2002 to 2006, during which he received the Henry Petersen Award, the Criminal Division's highest honor. Prior to coming to Washington, he served for nearly a dozen years as a Federal criminal trial prosecutor, and held a number of supervisory positions in the United States Attorney's Office in South Florida. Mr. Sabin received his bachelor's and master's degrees from the University of Pennsylvania and his law degree from the New York University School of Law.

Now, Mr. Sabin, I'm going to hold you harmless for this, but our Justice Department is infamously belated in getting its statements to us. As I say, I'm not blaming you for that, but if you could take back to Justice—I'm looking forward to the next session of Congress now. If they could provide us with the written testimony in a more timely way, we would be appreciative.

Mr. SABIN. Yes, sir.

Mr. COBLE. We will not kill the messenger in this case, but if you could convey that, I would be appreciative to you.

Our third witness is Mr. James Martin, President and Founder of the 60 Plus Association, a seniors advocacy group. Under Mr. Martin's leadership, membership at 60 Plus has soared to over 500,000, and the Association has ranked saving Social Security for future generations among its top priorities. In addition to founding 60 Plus, Mr. Martin has helped organize and direct several other advocacy groups, including the National Conservative Political Action Committee and the Public Service Research Council. Mr. Martin received a bachelor's degree in journalism from the University of Florida where he won a William Randolph Hearst award for writing;

And, Mr. Martin, I know you've done a very commendable job with 60 Plus. I had no idea your membership had soared a half million. That speaks well for your leadership.

Our final witness is unknown to none of us on this panel, Mr. Phil Kiko, Chief of Staff and General Counsel for the House Committee on the Judiciary. Prior to taking his current position with the Committee, Mr. Kiko served first as Legislative Director and then as Chief of Staff in Congressman F. James Sensenbrenner's congressional office. He also worked as Associate Counsel for the Judiciary Subcommittee on Civil and Constitutional Rights, where he focused on proposed constitutional amendments, crimes, civil rights, FBI, and immigration issues. He has been instrumental in the Committee on the Judiciary's passing of the USA PATRIOT Act, legislation overhauling the INS, visa reform, Border Security Act, and the first Justice Department authorization in over 20 years. Mr. Kiko earned his undergraduate degree at Mount Union College and received his J.D. from the International School of Law, now known as the George Mason University School of Law.

Mr. Kiko, I'm amplifying my ignorance now, but tell me where Mount Union is located.

Mr. KIKO. Alliance, Ohio.

Mr. COBLE. I figured there was a Buckeye connection there somewhere.

Gentlemen, we've been joined by the gentleman from Ohio, Mr. Chabot, and the gentleman from Florida, Mr. Keller, and no one on the minority side yet.

Gentlemen, we traditionally operate under the 5-minute rule here. When the amber light appears on your panel, that is your warning that you're running out of time. You'll have a minute to go at that point, and no one will be assaulted if you violate the 5-minute rule, but when the red light appears, the 5 minutes have elapsed, and at that point if you could wrap up, we would be appreciative.

I'm going to start with Mr. Murphy. Good to have you with us today.

TESTIMONY OF THE HONORABLE TIM MURPHY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF PENNSYLVANIA

Mr. MURPHY. Thank you, Mr. Chairman and Mr. Scott and Members of the Subcommittee. I appreciate an opportunity to discuss this bill H.R. 5304, the Preventing Harassment through Outbound Number Enforcement Act, or the PHONE Act; or, in this case, the PHONE bill.

Identity theft has become an increasingly critical problem for consumers. The Federal Trade Commission revealed earlier this year that 10 million individuals are the victims of identity theft each year, and identity theft is the number one consumer complaint in each of the 50 States. The disastrous implications of identity theft for consumers include damaged credit and financial ruin, and the effects can tear apart families.

Congress has repeatedly tried to prevent identity theft. Unfortunately, with new technology comes new risk and new opportunities for criminals to skirt the law. One of these technologies used by thieves is the practice of call spoofing, or caller ID fraud, where one masks their identity by altering the outbound caller ID number in order to mislead the call recipient. Some may describe call spoofing as a way to maintain caller privacy, but it is nothing less than fraud when used maliciously. That is because accountability is critically important in our judicial system. Caller ID fraud takes away accountability from people who wish to do harm to others.

Consider the effects of the false use of caller ID in other areas. Past Federal and State efforts to block unwanted phone solicitation with "do not call" lists was to provide some privacy for citizens, but when someone hijacks your phone number, they can bypass that protection.

I believe Congress must enact a law to penalize caller ID fraud perpetrators. This bill is particularly necessary to protect American families, the elderly and businesses because illegally using another person's phone number could have limitless unlawful applications.

It doesn't take much imagination to understand how dangerous this practice could be for unlawful people. A criminal could try to obtain personal financial information from individuals by using a bank's phone number. An ex-spouse could harass a former wife or husband who has blocked calls from the ex-spouse's phone line. A

pedophile could stalk a child by stealing a school phone number or the phone number of a friend of the child. A sexual predator could use a doctor's office phone number. A terrorist could make threats from a Government phone number. The list goes on.

The criminal use of caller ID fraud is not just a possibility, however. Here are some real-world examples of caller ID fraud that are very real and very disturbing. The AARP Bulletin reported a case in which people received calls that made false claims that they missed jury duty. To avoid prosecution, these individuals were asked for their Social Security number and other personal information. The phone number that appeared on their caller ID was from the local courthouse, so people assumed the caller was telling the truth.

The security company, Secure Science Corporation, has stated that criminals have accessed legal call spoofing Internet sites in order to protect their identities while they buy stolen credit card numbers. These individuals call a money transfer service such as Western Union and use a fake caller ID and a stolen credit card number to order cash transfers to themselves.

In 2005, SWAT teams surrounded an empty building in New Brunswick, New Jersey after police received a call from a woman who said she was being held hostage in an apartment. She was not in the apartment, and the woman had intentionally used a false caller ID. Imagine what might have happened.

For these reasons, I have introduced H.R. 5304 to punish those who engage in the intentional practice of misleading others through caller ID fraud. Violators of the bill would be subject to a penalty of up to 5 years in prison and up to $250,000 in fines. Unfortunately, pursuing these criminals is difficult and particularly resource-intensive. The House has already expressed its will on this matter, unanimously passing H.R. 5126, the Truth in Caller ID Act, which I have cosponsored, but this bill only asks the Federal Communications Commission to create a rule to prohibit caller ID fraud in 6 months. There are no penalties in the bill, and it doesn't stop people from skirting that law and still doing this. The Senate has not acted on H.R. 5126, and so the problems remain.

I also include an amendment to prompt the FCC to address the practice of caller ID fraud in H.R. 5672, the Fiscal Year 2007 Science, State, Justice, Commerce Appropriations Act. Still, I believe my bill, H.R. 5304, appropriately goes further by amending criminal law to fully protect Americans from the practice of caller ID fraud.

Over the years, Congress has been criticized as a reactive institution. Today, this Subcommittee is proactively considering a good idea that addresses a problem before a tragedy occurs. Today, we have a chance to help stop crime, prevent identity theft and protect lives.

Thank you for your commitment to the personal identity security of all Americans, and I would be happy to answer any questions you may have. Thank you, Mr. Chairman.

Mr. COBLE. And you have applied pressure to your colleagues because you beat the red light, Mr. Murphy. I commend you for that.

[The prepared statement of Mr. Murphy follows:]

PREPARED STATEMENT OF THE HONORABLE TIM MURPHY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF PENNSYLVANIA

Mr. Chairman, Ranking Member Scott, distinguished colleagues of the Committee, thank you for inviting me to speak before you today on behalf of my legislation, H.R. 5304, the Preventing Harassment through Outbound Number Enforcement Act, or the PHONE Act.

Identity theft has become an increasingly critical problem for consumers. The Federal Trade Commission revealed earlier this year that 10,000,000 individuals are victims of identity theft each year, and identity theft is the number one consumer complaint in each of the fifty states. The disastrous implications of identity theft for consumers include damaged credit and financial ruin, and the effects can tear apart families.

Congress has repeatedly tried to prevent identity theft. Unfortunately, with new technology comes new risks and new opportunities for criminals to skirt the law. One of these technologies used by thieves is the practice of "call spoofing," or "caller ID fraud," where one masks their identity by altering their outbound caller ID number in order to mislead the call recipient. Some may describe call spoofing as a way to maintain caller privacy. But it is nothing less than fraud. That's because accountability is critically important in our judicial system. Caller ID fraud takes away accountability from people who wish to do harm to others.

Stealing, masking or otherwise altering one's caller identification to deceive is a new tool in the hands of criminals. The practice of caller ID fraud can be tremendously harmful to consumers.

Consider the effects of the false use of caller ID in other areas. Past federal and state efforts to block unwanted phone solicitations with "Do Not Call" lists was to provide some privacy for citizens. But when someone hijacks your phone number, they can bypass that protection.

I believe Congress must enact a law to penalize caller ID fraud perpetrators. This bill is particularly necessary to protect American families, the elderly and businesses, because illegally using another person's phone number could have limitless unlawful applications. It doesn't take much imagination to understand how dangerous this practice could be for unlawful people:

- A criminal could try to obtain personal financial information from individuals by using a bank's phone number,
- An ex-spouse could harass a former wife or husband who has blocked calls from the ex-spouse's phone line,
- A pedophile could stalk a child by stealing a school phone number or the phone number of a friend of the child,
- A sexual predator could use a doctor's office phone number, or
- A terrorist could make threats from a government phone number.

The criminal use of caller ID fraud is not just a possibility. Here are some real world examples of caller ID fraud that are real and very disturbing:

•

The AARP Bulletin reported cases in which people received calls that made false claims that they missed jury duty. To avoid prosecution, these individuals were asked for their Social Security number and other personal information. The phone number that appeared on their caller ID was from the local courthouse, so people assumed the caller was telling the truth.

- The security company, Secure Science Corporation, has stated that criminals have accessed legal call spoofing Internet sites in order to protect their identities while they buy stolen credit card numbers. These individuals call a money transfer service such as Western Union and use a fake Caller ID and a stolen credit card number to order cash transfers to themselves.
- In 2005, SWAT teams surrounded an empty building in New Brunswick, New Jersey, after police received a call from a woman who said she was being held hostage in an apartment. She was not in the apartment, and the woman had intentionally used a false caller ID. Imagine what might have happened.

For these reasons, I have introduced H.R. 5304 to punish those who engage in the intentional practice of misleading others through caller ID fraud. Violators of the bill would be subject to a penalty of up to five years in prison and fines of $250,000. Unfortunately, pursuing these criminals is difficult and particularly resource intensive.

The House has already expressed its will on this matter, unanimously passing H.R. 5126, the Truth in Caller ID Act, which I have cosponsored. But this bill only

asks the Federal Communications Commission to create a rule to prohibit caller ID fraud in six months. There are no penalties in the bill. The Senate has not acted on H.R. 5126, and so the problems remain. I also included an amendment to prompt the FCC to address the practice of caller ID fraud in H.R. 5672, the Fiscal Year 2007 Science, State, Justice, Commerce Appropriations Act. Still, I believe my bill, H.R. 5304, appropriately goes further by amending criminal law to fully protect Americans from the practice of caller ID fraud.

Over the years, Congress has been criticized as a reactive institution. Today, this subcommittee is proactively considering a good idea that addresses a problem before a tragedy occurs. Today we have a chance to help stop crime, prevent identity theft and protect lives.

Thank you for your commitment to the personal identity security of all Americans. I would be happy to answer any questions you might have.

Mr. COBLE. Mr. Sabin.

TESTIMONY OF BARRY SABIN, DEPUTY ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, UNITED STATES DEPARTMENT OF JUSTICE

Mr. SABIN. Good morning, Mr. Chairman, Ranking Member Scott, and Members of the Subcommittee. It is my pleasure to appear before you today to discuss H.R. 5304, the Preventing Harassment through Outbound Number Enforcement Act.

The United States Department of Justice supports congressional action such as the PHONE Act to provide law enforcement better tools to protect our citizens and our countries from identity thieves, stalkers, fraudsters, and other criminals. The phone Act targets caller ID spoofing. That is the falsifying of information transmitted by the telephone network that causes a call recipient's caller identification equipment to display incorrect information about who is calling. Recent changes in technology, particularly Voiceover Internet Protocol equipment, have made caller ID spoofing relatively easy and inexpensive. As a result, services available through the Internet or through toll-free telephone numbers have brought caller ID spoofing to the mainstream. These services allow users to have placed calls while enabling the user to choose any number they wish to appear on their recipients' caller ID displays. There is no meaningful way for consumers to opt out of receiving spoofed calls or to prevent their telephone numbers from being spoofed.

While this technology is relatively new, we are already seeing it being misused. Criminals can use caller ID spoofing to facilitate a number of crimes, including identity theft, harassment, privacy invasions, and other types of fraud. Caller ID spoofing can assist a criminal to trick an individual into providing a credit card number or a Social Security number or to fool a domestic abuse victim into accepting a harassing call. Identity thieves, hackers and other criminals also can use caller ID spoofing to circumvent security measures put in place by financial institutions, communication service providers and others. These concerns are not theoretical. We know that criminals are using these caller ID spoofing services to further their crimes today.

The crux of the crime is the criminal's intent to mislead. For instance, James Turner Hopper recently pleaded guilty to several Federal felony offenses, including identity theft. Mr. Hopper was able to use caller ID spoofing more than 150 times in order to hide his true identity and to defeat security controls while attempting to steal over $88,000. Hopper was recently sentenced to 30 months'

incarceration in the United States District Court for the Southern District of California.

The Justice Department is concerned with the widespread availability of caller ID spoofing services that present significant potential for abuse and hinder law enforcement's ability to timely and thoroughly investigate crime. We believe that this matter merits further study and suggests that Congress consider whether a civil or criminal prohibition on caller ID spoofing services in appropriate circumstances would be warranted. We would be happy to work with the Committee and Subcommittee in exploring the issue further.

In addition, the Justice Department has a variety of suggestions to clarify and strengthen the bill that will be provided to the Subcommittee shortly. Among other recommendations, DOJ suggests that the drafters consider a more graduated series of offenses that would allow prosecutors to charge a full range of misdemeanor and felony offenses as well as forfeiture provisions in appropriate circumstances. The Department of Justice appreciates this Subcommittee's proactive leadership in making sure that our country's laws meet this new challenge.

Thank you for the opportunity to testify today and for your continuing support. I am happy to answer any questions you may have.

Mr. COBLE. Mr. Sabin, you, too, were very disciplined in beating the red light.

[The prepared statement of Mr. Sabin follows:]

PREPARED STATEMENT OF BARRY SABIN

STATEMENT

OF

BARRY SABIN
DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION
U.S. DEPARTMENT OF JUSTICE

BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY
COMMITTEE ON THE JUDICIARY
U.S. HOUSE OF REPRESENTATIVES

CONCERNING

"LEGISLATIVE HEARING ON H.R. 5304,
THE 'PREVENTING HARASSMENT THROUGH OUTBOUND NUMBER ENFORCEMENT (PHONE) ACT'"

PRESENTED ON

NOVEMBER 15, 2006

Statement of Barry Sabin
Deputy Assistant Attorney General
Criminal Division, U.S. Department of Justice
Before the U.S. House of Representatives
Committee on the Judiciary
Subcommittee on Crime, Terrorism, and Homeland Security

Concerning

H.R. 5304, Preventing Harassment through Outbound Number Enforcement Act

November 15, 2006

I.

Introduction

Good morning, Mr. Chairman, Ranking Member Scott, and Honorable Members of the Subcommittee. It is my pleasure to appear before you to discuss H.R. 5304, the "Preventing Harassment through Outbound Number Enforcement Act (PHONE Act)." The United States Department of Justice supports Congressional action such as the PHONE Act to give law enforcement better tools to protect our citizens and our country from identity thieves, stalkers, and other criminals.

This bill targets a telephone calling practice known as "caller ID spoofing." Caller ID spoofing is the modification of caller ID information that causes the telephone network to display a number and other information on the recipient's caller ID display that is not the number of the actual caller.

Recently, caller ID spoofing services have become widely available, greatly increasing the number of people who have access to this tool to deceive others. By outlawing the misuse of caller ID spoofing, the PHONE Act, with modifications we will recommend today, can

improve the Department's ability to prevent crimes ranging from identity theft to harassment to pretexting.

II.

Caller ID Spoofing Is Being Used By Criminals To Commit Crimes Such as Identity Theft and to Invade Americans' Privacy.

Criminals can use caller ID spoofing to facilitate a number of crimes, including identity theft, harassment, privacy invasions, and even election fraud. Obviously, caller ID spoofing can help to hide the identity of a criminal, but it can go farther, actually defeating security measures that would have prevented a crime.

For example, caller ID spoofing can lend credibility to a criminal trying to trick an individual into giving up private information, such as a credit card number or social security number. By making it appear that the call is coming from a legitimate charity or bank, from a business's customer, or even from the office of a political campaign, a victim can be more easily fooled into giving up private information. For instance, a "pretexter" can call telephone companies pretending to be a subscriber and try to obtain the subscriber's private telephone records. If the caller ID information matches the subscriber's home telephone number, the pretexter can more easily gain access to those private records.

Caller ID spoofing can also create opportunities for abusers who could not otherwise contact their victims to reach into those victims' homes and further harass them. Misleading caller identification information could cause a victim to accept a call they would otherwise avoid or circumvent automatic call-blocking that would have prevented the harassing call from being connected.

Identity thieves, hackers, and other criminals might also use caller ID spoofing to circumvent security measures put in place by financial institutions, money transfer agents,

communication service providers, retailers, and restaurants. Such businesses sometimes use caller ID information as part of their fraud prevention measures as a way of confirming the identity of the caller. If the information fed into these systems is inaccurate, the security measures might be defeated and allow transactions or access to private information that would otherwise have not been permitted.

These concerns are not theoretical; we know that criminals are using these caller ID spoofing services to further their crimes today. Take, for instance, the case of James Turner Hopper, who pleaded guilty to several federal felony offenses involving identity theft. Hopper admitted that he obtained over 100 credit card numbers and associated identity information. He then placed calls to a money transfer agent and used the stolen credit card accounts to send money to himself and others. To make these calls, Hopper used a caller ID spoofing service in order to hide his true identity and to defeat internal security controls that would have disclosed that he was using other peoples' credit card numbers. Hopper was able to use this tactic more than 150 times while attempting to steal over $88,000. The United States District Court for the Southern District of California recently sentenced Hopper to 30 months in prison.

III.

Caller ID Spoofing Services Have Become Widespread and Readily Available to the Public.

Recent changes in technology have made caller ID spoofing much easier and less expensive, which has led to services that allow many who would otherwise lack the necessary technical sophistication or equipment to spoof caller ID to be able to do so from any telephone or Internet connection.

Widely available Voice-over-Internet-Protocol (VOIP) equipment can easily be

configured to populate the caller ID field with information of the user's choosing. Equipment owners can easily allow users to connect to their equipment through the Internet or through toll-free telephone numbers. Once connected to the spoofing service, users can connect to any other telephone and choose what telephone number they wish to transmit to their recipients. Numerous spoofing services exist today that allow anyone to change his or her caller ID information simply by placing a call through a toll-free number or by setting up the call through the Internet.

It is the widespread availability of these new services that has brought caller ID spoofing to the mainstream. While this development is relatively new, we are already seeing that the capability is being misused to facilitate crimes and could be used to hamper investigations.

Addressing the problem, of course, must be done carefully. We understand that modifications to caller ID information can be done for benign or even beneficial purposes. There are instances where caller ID information is modified to accurately reflect the calling party, such as in call forwarding or to meet the requirements of emergency telecommunications, such as E911. These are functions undertaken by the telephone companies where no one is misled as to the true calling party.

It has been claimed that caller ID spoofing serves to protect people's privacy. The PHONE Act already wisely preserves as an option for telephone users to use caller ID blocking, *i.e.*, preventing your number from being known. Simply put, the caller gets to make a choice about whether to reveal his or her number and the recipient gets to make a decision about whether to take the call.

Some have further suggested that, as an alternative to blocking caller ID information,

individuals would benefit from being able to modify caller ID information in order to provide alternative call-back information. While this could in some instances be a non-objectionable use, today, there is no requirement that providers of caller ID spoofing services make any effort to verify that the person requesting to place a call with altered caller ID has any right to use the number requested. This lack of verification provides opportunities for misuse.

Moreover, the widespread availability of caller ID spoofing services could complicate criminal investigations. For example, if kidnappers or terrorists were to use caller ID spoofing, law enforcement involved in fast-moving investigations could lose valuable time chasing down the wrong path.

IV.

H.R. 5304 Could Be Improved to More Effectively Combat the Harms Caused by Widely Available Caller ID Spoofing.

The Department is concerned with the widespread availability of caller ID spoofing services that present significant potential for abuse and hinder law enforcement's ability to investigate crime. We believe that this matter merits further study, and suggest that Congress consider whether a civil or criminal prohibition on caller ID spoofing services in appropriate circumstances would be warranted. We would be happy to work with the Subcommittee in exploring the issue further.

Overall, the bill supports the Department's efforts to combat the threats caused by caller ID spoofing. The Department was pleased to see that the scope of the bill includes both conventional telephone calling and many types of VOIP services. The drafters have also wisely recognized that, at times, it may be necessary to modify caller ID information in the course of authorized law enforcement and intelligence operations. Accordingly, the bill properly includes an exception for these legitimate law enforcement and intelligence

activities.

The Department has a number of other recommendations to clarify and strengthen the bill and to make it more effective.

A. The bill could be made more effective by creating a more graduated series of offenses rather than just a felony charge.

Subsection (a) would subject violators of the proposed law to fines or imprisonment or both, but creates only one felony offense. A felony is a very serious charge that carries heavy penalties that may not be proportional to the conduct at issue in every case. The drafters may wish to consider a more graduated series of offenses that would allow prosecutors to charge misdemeanor offenses in appropriate circumstances. For instance, felony penalties could be reserved for caller ID spoofing done in furtherance of another crime or tort, while other conduct could be reduced to the level of a misdemeanor offense. This could lead to greater use of the statute and more just results. Such an approach has been implemented in other federal criminal statutes such as 18 U.S.C. § 1030(c)(2)(B) (part of the Computer Fraud and Abuse Act) and 18 U.S.C. § 2701(b) (the criminal provision in the Electronic Communications Privacy Act). We suggest below language based on 18 U.S.C § 2701.

B. The bill could be made more effective by prohibiting attempts.

A prosecution should not depend on whether a criminal was successful in the object of his crime. Thus, if a call placed by a criminal attempting to mislead another does not connect for some reason, the criminal should be punishable as if the call had been completed. Such failures may occur, for example, where a service has blocked certain numbers, such as 911, or even for more mundane technical problems. Thus, we recommend that the bill punish attempts the same as the substantive offense.

C. The bill could be made more effective by incorporating technical changes.

The Department proposes a variety of changes that we believe will clarify the bill. Among other recommendations, these changes include a statement of jurisdiction, using technology-neutral terminology, and including a forfeiture provision. In a separate letter, we will pass on these suggestions to you, along with the Department's recommended edits to the bill.

V.

Conclusion

The Department of Justice appreciates this Subcommittee's leadership in making sure that our country's laws meet this new challenge. Thank you for the opportunity to testify today and for your continuing support. I am happy to answer any questions you may have.

Mr. COBLE. Mr. Martin, the pressure is upon you now.

TESTIMONY OF JAMES MARTIN, PRESIDENT AND FOUNDER, 60 PLUS ASSOCIATION

Mr. MARTIN. Thank you, Mr. Chairman, and Mr. Chairman to be. I appreciate the opportunity here to offer some comments. And by the way, I need to update my biographical sketch. That 500,000 has grown 10 years ago to about 5 million now and is still growing. We're not nearly with the AARP, but we're getting there.

Incidentally, my honorary chairman is a former colleague of yours, Roger Zion of Evansville, Indiana. Hale and hearty at 85 years young, Roger was elected to the 90th Congress in 1966 and served with distinction here for 4 consecutive terms.

I'm also proud of the fact that our National spokesman is none other than the legendary entertainer Pat Boone. In the Top 10 all-time of recording artists, nobody but nobody sold more records in the fifties and sixties than Pat, except for a fellow by the name of Elvis.

I don't want to attempt to have you believe that I am an expert on spoofing or phishing. That's "phishing" spelled with a P-H, by the way, not the way that we spell the recreational activity that so many of us "gray hairs" like myself enjoy; but in a sense, that's why we're here, isn't it? Things aren't always what they seem in this brave new world of high-tech, and we seniors accept that it's the progress that it represents. What we're not about to accept is fraud, deceit, larceny, character assassination, and identity theft. We didn't accept it back in the fifties when the guy selling aluminum siding left us holding the bag. We didn't, in recent years, as telephone scams were perfected, and we won't now with cyberspace being manipulated for the same ends: greed.

This matter of spoofing or phishing strikes me as serious business. Just as seniors are beginning to get computer literate, we've learned some basics like with spam. Over time, we've learned it's garbage via e-mail that we didn't ask for, and as an unwanted document, we can merely delete the file. It's a pain in the neck, but it isn't lethal. But with phishing, a senior logs onto their e-mail account and is duped by use of a legitimate name or vendor that they may have an actual account with—say, the bank or credit card—and since they're likely to want to access the information, they click onto a link or otherwise take action and fill out personal information, something they innocently believe is an update, but it's really designed to give the phishers personal information that could be lethal.

This matter of spoofing strikes me as a new low. Someone receives an e-mail from a friend or a loved one. Surely, anyone would open that message, right? Well, hold on. It turns out with spoofing, a virus attacks your address book or seizes addresses from your "to" and

from" field and manipulates it in such a way that you're either sending or receiving a knockout blow of a virus. This is bad stuff.

It's much the same for the telephone. Let's say you're paying for a service we all know, called "caller ID". Well, be careful. The number you recognize as your Aunt Betty's number really isn't hers. The bad guys spoofed poor Aunt Betty and grabbed her number to

mask the bad guy's real number. And lo and behold, you pick up, and the connection is made, like it or not. It could be a telemarketing scam. It could be just about anything. It's bad stuff.

As more seniors get Internet savvy, as telephones and cell phones become smart phones, the opportunity to be scammed only goes up. We at 60 Plus have not received what you might consider an alarming number of complaints on this issue, but it's only a matter of time. This is a stink that's coming, and we want to be proactive. So, for example, in the next edition of our national quarterly magazine, Senior Voice, I plan to post this very testimony and publicize these important hearings. But let's face it: While we seniors have slowed down some, we still would like to think we're quick enough to handle the telephone or surf the Net with some dispatch. Now, we have a right to expect fair play on the other end. If not, then we have a legitimate right to ask our elected officials to step up to the plate and do the right thing—pass tough, no-nonsense laws that severely penalize those who would wish us harm.

In closing, seniors are shut-ins, sometimes connected to the outside world by the phone and now, increasingly, by the Internet. They're alone and they're lonely and they're easy victims. It's my hope that this Committee will do whatever is necessary to ensure that scammers get nailed for stealing seniors' passwords, user names, bank information, credit card data, and more.

Thank you for your compassion, and while my time is not up, I sincerely thank you for yours.

Mr. COBLE. I confess ignorance and embarrassment, Jim. We were taking the 500,000 from your bio, and I didn't even realize that there were 500,000, much less 5 million, but I commend you for that, and I wish—I think I speak for Bobby. I want you to convey good wishes to Roger and to Pat Boone, if you will.

[The prepared statement of Mr. Martin follows:]

PREPARED STATEMENT OF JAMES L. MARTIN

Good morning, I'm Jim Martin, President of the 15-year-old-and-counting 60 Plus Association[1] and I appreciate the invitation to offer comments today on behalf of some 5 million senior citizens we call upon for support. For the record, I have prepared remarks and I'll now summarize: incidentally, my Honorary Chairman is a former colleague of yours, Roger Zion of Evansville, Indiana. Hale and hearty at 85 years young, Roger was elected to the 90th Congress in 1966 and served four consecutive terms. I'm proud of the fact that our national spokesman is none other than the legendary entertainer, Pat Boone. In the Top 10 all-time of recording artists, nobody but nobody sold more records in the 50s than Pat except for a fellow named Elvis.

I don't stand here today attempting to have you believe I'm an expert on "spoofing" or "phishing" . . . that's fishing spelled with a "ph", by the way, not the way I'm accustomed to spelling the recreational activity so many "gray hairs" like myself enjoy.

But you know, in a sense, I suppose that's what we're here about now, isn't it? Things that aren't really what they seem. Fishing spelled with a "ph". "Mac" not being your golfing buddy but a computer system. "Windows" not being what you

[1] The 60 Plus Association is a 15-year-old nonpartisan organization taking on important issues such as death tax repeal, saving Social Security, working to lower energy costs, affordable prescription drugs and other senior-friendly issues featuring a less government, less taxes approach. 60 Plus calls on support from nearly 4.5 million citizen activists. 60 Plus publishes a quarterly magazine, SENIOR VOICE, and a Scorecard, bestowing a Guardian of Seniors' Rights award on lawmakers of both parties who vote "pro-senior." 60 Plus has been called "an increasingly influential senior citizen's group." 60 Plus has established a membership benefit program. To join 60 Plus or for further information, please go to our website at *www.60plus.org* or call 888-560-PLUS (7587).

clean each spring but rather what has made Bill Gates a household name. "Wallpaper" that has nothing whatever to do with walls; "bugs" having nothing to do with insects; and a "cursor" having nothing to do with inappropriate language.

And don't even ask me about iPods and Bluetooths or Boysenberries . . . or is that Blackberry's?

You see, the old warhorse that I am, I know that things ain't always what they seem in this brave new world of hi-tech. And we seniors are prepared to accept that for the great rush of progress that it represents. But what we're NOT about to accept is fraud, deceit, larceny, character assassination and identity theft. We didn't back in the 1950s when the guy selling aluminum siding left us holding the bag . . . we didn't in recent years as telephone scams were perfected . . . and we won't now with cyberspace being manipulated for the same ends: greed.

This matter of "spoofing" or "phishing" strikes me as very serious business. Just as we seniors are beginning to get computer literate, we've learned some basics: like with "spam"—over time we've learned that it's garbage via email that we didn't ask for and as an unwanted document, we can merely delete the file. It's a pain in the neck, but it isn't lethal.

But with "phishing," a senior logs on to their email account and is duped by use of a legitimate name or vendor that they may have an actual account with—say the bank or MasterCard or eBAY—and since they're likely to want to access the information, they click on to a link or otherwise take action and fill-out personal information—something they innocently believe is an update—but is really designed to give the "phishers" personal info that indeed could be lethal!

Or take this matter of "spoofing" . . . this strikes me as a new low! Someone receives an email from a friend or loved one . . . well surely, anyone would open that missive, right? Well, hold on! Turns out with "spoofing," a virus attacks your address book or seizes addresses from your TO and FROM fields and manipulates it in such a way that you are either sending or receiving a knock-out blow of a virus! Very bad stuff, for certain.

And it's much the same for the telephone . . . let's say you're paying for a service we all know called Caller ID. Well careful, now the number you recognize as your Aunt Betty's number really isn't hers! The bad guys "spoofed" poor Aunt Betty and grabbed her number to mask the bad guy's real number and lo and behold, you pick up and the connection is made, like it or not. Could be a telemarketing scam, could be pornography, could be just about anything! Bad stuff!

I'm an old direct mail guy . . . snail mail, if you will . . . and after 40 years, probably know as much or more about the direct mail business as most. Could the direct mail business get pretty shoddy? Of course it could BUT the recipient wasn't electronically connected; and they were in the privacy of a home or office, able to dispose of the literature opened or unopened and the matter was over and done with. That's not the way today. And as more of my seniors with 60 Plus get "Internet" savvy, as telephones and cell phones become "smartphones" and ooze into every facet of our personal and business lives, the opportunity to be scammed only goes up.

I'll be perfectly candid with you here: we at 60 Plus have not received what you might consider an alarming number of complaints on this issue. But it's only a matter of time. This is a stink that's coming and we want to be proactive. So, for example, in the next edition of our national quarterly magazine, Senior Voice, I plan to post this very testimony I'm delivering today and publicize these important hearings.

But let's face it, while we seniors have slowed down some, we still would like to think we're quick enough to handle the telephone or surf the Net with some dispatch—and we have a right to expect fair play on the other end. If not, then we have a legitimate right to ask our elected officials to step up to the plate and do the right thing: pass tough, no-nonsense laws that severely penalize those who would wish us harm.

In closing, I'll tell you testifying at events like these make me pretty hungry. I don't mind telling you I'm looking forward to lunch this afternoon; I'm going to have some "Spam" . . . the food staple I've known for decades . . . followed by a few "bytes" of a some "cookies" . . . really, munch down on some Oreos . . . brought to me by a "server" . . . you know, a real waiter . . . and I'll wash it all down with some "Java" . . . honest-to-God coffee!

Well, there's my two "bits" . . . pun intended.

Seriously, I thank you for your allowing 60 Plus to weigh in on this important matter to seniors. It's my hope that this committee will do whatever is necessary to ensure the scammers get nailed for stealing senior's passwords, usernames, bank information, credit card data and more.

I'd also be remiss if I didn't mention how I appreciate Rep. Tim Murphy (R-PA) introducing this important legislation . . . H.R. 5304, the Preventing Harassment through Outbound Number Enforcement Act . . . and acknowledge his consistent service to senior citizens, observing he served as Chair of the Pennsylvania Committee on Aging when he was in the state Senate there.

Well, I see my time is up . . . I thank you, most sincerely, for yours.

Mr. COBLE. And as an aside, Mr. Scott, I don't think I remember a single hearing where all four witnesses beat the red light, so the pressure is on Mr. Kiko.

The gentleman is recognized for 5 minutes.

TESTIMONY OF PHIL KIKO, GENERAL COUNSEL AND CHIEF OF STAFF, COMMITTEE ON THE JUDICIARY, UNITED STATES HOUSE OF REPRESENTATIVES

Mr. KIKO. Yeah. I guess I'd better comply with the Chairman's rule; is that correct? All right.

Good morning, Chairman Coble, Ranking Member Scott and Members of the Subcommittee. I thank you for the opportunity to testify regarding the need to pass H.R. 5304, legislation which criminalizes spoofing, the act of modifying telephone caller identification information with the intent to mislead the recipient as to the identity of the actual caller. I appear before you this morning as a victim who has experienced firsthand the invasion of my personal privacy and information and the frustration caused by spoofing.

Spoofing creates two categories of victims: first, the person who receives the telephone call identified as coming from someone other than the actual caller; and, two, the person whose caller identification is used fraudulently to disguise the true identity of the caller.

I fall into the second category, because without our family's knowledge or consent, my caller identification was used, obviously hundreds of times, to mask the true identity of a fraudulent caller. As a result, my family and I received up to 20 phone calls a day over a several months' period of time from people who fall into Category 1, who were either returning the telephone call of a fraudulent caller, asking me to stop calling them, or asking me to take them off the telemarketing list.

However, the harm to the victims of spoofing does not end with being inundated with, you know, daily and unwanted telephone calls.

The impact of spoofing on victims is compounded by the fact that it is extremely difficult for victims, and apparently for the telephone companies and for anyone else, to identify the source of and the names of individuals placing the fraudulent telephone calls or to prevent the victim's caller ID from being circulated to other fraudulent callers working off mass mailing or telemarketing lists. Thus, even if the original fraudulent caller is identified, there's a high probability that the victim's information will already have been forwarded multiple times to other unscrupulous callers and telemarketers. In some instances, the minutes used for fraudulent telephone calls have been charged to the victim's telephone plans. As a result, the negative impact on the victim never ends but, instead, only snowballs and gets worse.

Currently, the victims of spoofing have little or no recourse against those who spoof. The only effective way to end being vic-

timized is to change one's telephone number, at a great inconvenience, due in part to the infrastructure and technical operations of the telephone companies.

In an attempt to put a stop to the never-ending and unwanted phone calls to my house and to stop my caller ID from being used to facilitate fraudulent calls, we contacted the telephone company to inquire as to our options. To our frustration, my wife's and my frustration, we were informed that we could not prevent our caller ID from being used to facilitate spoofing. Instead, the only way our caller ID would not be used is if the recipient of the call contacted the telephone company requesting that all calls from our caller ID be blocked. Thus, the only way our caller ID would be totally stopped from being fraudulently used is if every single person who received a fraudulent phone call contacts the telephone company and requests that calls to our caller ID be blocked, a highly unlikely scenario, especially in light of the fact that our caller ID will have most likely been passed on to other fraudulent callers.

Ultimately, like so many other victims of spoofing, we were left with the only effective option of changing the telephone number that our family and I have had for 16 years. This has obviously been a significant inconvenience. But even changing our telephone number is no guarantee that we will not be victims of spoofing again, because the bad actors could obtain our new telephone number and the violations would start all over.

In conclusion, spoofing has no valid social or economic purpose, and it is a serious problem. Our family has experienced firsthand the invasion of privacy and inconvenience and frustration, and sometimes harassment, from spoofing, but we have heard very compelling testimony from the other witnesses at this table about the criminal aspects regarding spoofing.

So I want to thank the Subcommittee for holding a hearing on H.R. 5304, the PHONE Act, which will help reduce and hopefully eliminate the harmful activity of spoofing. Thank you very much.

Mr. COBLE. Thank you, Mr. Kiko.

[The prepared statement of Mr. Kiko follows:]

PREPARED STATEMENT OF PHIL KIKO, ESQUIRE

INTRODUCTION

Good morning, Chairman Coble, Ranking Member Scott, and Members of the Subcommittee. My name is Phil Kiko and I thank you for the opportunity to appear before you this morning, to testify regarding the need to pass H.R. 5304, legislation which criminalizes Spoofing, the act of modifying telephone caller identification information with the intent to mislead the recipient as to the identity of the actual caller. I appear before you this morning to testify as a victim who has experienced first hand the invasion of my personal privacy and information, the harassment, and the frustration caused by Spoofing.

TESTIMONY

The act of Spoofing creates two categories of victims: 1) the person who receives a telephone call identified as coming from someone other than the actual caller; and 2) the person whose caller identification is used fraudulently to disguise the true identity of the caller. I fall into the second category, because without my knowledge or consent, my caller identification ("ID") was used hundreds, if not thousands, of times to mask the true identity of a fraudulent caller. As a result, my family and I have received up to 20 telephone calls a day from angry people who fall into category one, who were either: returning the telephone call of the fraudulent caller;

asking me to stop calling them; or asking me to take them off the telemarketing list.

However, the harm to the victims of Spoofing does not end with being inundated daily with unwanted telephone calls. The impact of Spoofing on victims is compounded by the fact that it is extremely difficult for the victims (and apparently for the telephone companies and for anyone else) to identify the source of, and or the names of individuals placing the fraudulent telephone calls; or to prevent the victim's caller ID from being circulated to other fraudulent callers working off of mass-mailing or telemarketing lists. Thus, even if the original fraudulent caller is identified, there is a high probability that the victim's information will have already been forwarded multiple times to other unscrupulous callers and telemarketers. In some instances, the minutes used for fraudulent telephone calls have been charged against the victim's telephone plans. As a result, the negative impact to the victim never ends, but instead only snowballs and gets worse and worse.

Currently, the victims of Spoofing have little or no recourse against those who Spoof. The only effective way to end being victimized is to change one's telephone number—a great inconvenience; due in part to the infrastructure and technical operations of the telephone companies.

In an attempt to put a stop to the never-ending harassment and annoyance of unwanted telephone calls to my house, and to stop my caller ID from being used to facilitate fraudulent calls: I contacted my telephone company to inquire as to my options. To my frustration, I was informed that I could not prevent my caller ID from being used to facilitate Spoofing. Instead the only way my caller ID would not be used, is if the recipient of the call contacted the telephone company requesting that all calls from my name and number be blocked. Thus, the only way my caller ID would totally be stopped from being fraudulently used is if every single person who receives a fraudulent call contacts the telephone company and requests that calls from my caller ID be blocked; a highly unlikely scenario, especially in light of the fact that my caller ID will have most likely been passed on to other fraudulent callers.

Ultimately, like so many other victims of Spoofing, I was left with only one effective option: changing the telephone number that my family and I have had for fifteen years. This has been a significant inconvenience, as my family and I had to inform our family, friends and employers of the number change, as well as those companies that provide basic services such as utilities and cable. But even changing our telephone number is no guarantee that we will not be a victim of Spoofing again, because the bad actors could obtain our new telephone number, and the violations start all over.

CONCLUSION

In conclusion, Spoofing, has no valid social or economic purpose, and is thus a serious problem. My family and I have experienced first hand the invasion of privacy, harassment, inconvenience and frustration caused by Spoofing.

I want to thank this Subcommittee for holding this hearing on H.R. 5304, the PHONE Act, which will help reduce and hopefully eliminate the harmful activity of Spoofing. I am happy to answer any questions.

Mr. COBLE. And, Mr. Scott, we failed to set a record. Mr. Kiko, the red light did illuminate just at the wrong time. We'll hold you harmless for that. Now, gentlemen, we also impose the 5-minute rule against ourselves as well. Let me start by putting a hypothetical to Mr. Murphy or to Mr. Sabin.

Mr. Murphy, let's assume that I'm going to move some furniture, and I know that Bobby Scott has a truck, and I know he's not going to be interested in loaning—in lending that truck to me, and he's going to avoid me. If I could ever contact him, I think he'll be obliged to give me his truck. I use Mr. Chabot's phone number, figuring he would accept Chabot's call. I get him on the phone, and then I put my question to him, and Bobby reluctantly loans the truck to me, but voluntarily. Now, have I committed a crime under your bill, Mr. Murphy or Mr. Sabin?

Mr. MURPHY. No, I don't believe that is a crime under these circumstances and certainly would be willing to work with the Com-

mittee and the Justice Department to make sure we clearly define that, because what happened there is you did not commit a crime. However, if you used another phone number to access private information—a Social Security number, credit card numbers, et cetera—then it goes in that category.

What I see as the importance of this bill is really adding a penalty when you use the phone and the phone spoofing to commit a crime.

Mr. COBLE. Well, in my hypothetical, Mr. Scott really has lost nothing. He voluntarily relinquished the use of the truck, but he wouldn't have done it if I'd used my phone number.

Mr. Sabin, what do you say to this?

Mr. SABIN. Currently, under Federal law, spoofing is not a Federal crime. It can be critical as a means for trying to accomplish some kind of scheme to defraud or other types of illegality in certain circumstances, so we would address it through mail fraud, wire fraud, other kinds of fraud-based offenses. The key is the mens rea, the intent—the intent to mislead in order to seek to obtain some property or some kind of financial remuneration in certain circumstances, or harass or do other things in other circumstances.

So you could have a range of penalties from a misdemeanor, depending upon the kind of intent that you are seeking to accomplish, but based upon your factual circumstances, it certainly wouldn't be one that we would exercise prosecutorial discretion; nor, based upon your facts, would I think it would fall within the appropriate mens rea that it would be actionable under Federal law.

Mr. COBLE. That would be my hope, that even though I've committed fraud against Mr. Scott in the phone call, he's saying he suffered no damages except giving me the truck. Thank you for that.

We're going to probably have a second round of questions here, gentlemen, because my time is going to be up in a minute.

Mr. Martin, let me put a question to you. Does the act of spoofing take on similar traits as other scams perpetrated on the elderly; and, if so, what are other scams and similarities?

Mr. MARTIN. Yes, sir, I believe so, especially—like a few years ago. Coming over here, I recall I testified before one of the Subcommittees 7, 8, 9 years ago, on the telephone scams that were occurring with more frequency, and especially among the elderly, because as I said in my prepared remarks, the elderly are shut-ins, if you will, at home. Sometimes their only contact with the outside world is the telephone. And now, of course, as we get into the computer business, more and more relying on computers. But clearly, so many seniors live in a home, and they perhaps don't hear quite as well as they did some years ago, and they're lonely, quite frankly, and they're all alone, and so——

Mr. COBLE. And susceptible.

Mr. MARTIN. And very susceptible to these scams, and it's just—it's heartbreaking when you hear some of these cases. But I did testify a few years ago along those lines, and of course, this is something new. As I said in my remarks, it's not a pandemic yet, but it's certainly something that's on the horizon. And we thank Mr. Murphy for introducing this bill, and we thank, sincerely, this Committee for holding these hearings.

Mr. COBLE. Thank you, sir.

You may have mentioned this in your testimony, but were you able to determine who fraudulently used your caller ID, A; and, B, was the telephone company any help in determining how the fraudulent caller obtained your caller ID?

Mr. KIKO. No, we were never able to determine that, and the telephone company was not—they were unable, really, to pursue this or to be of much help other than to say we had to call—the other people that were calling, they were the ones that had to call to stop the number.

Mr. COBLE. The distinguished gentleman from Virginia, Mr. Scott.

Mr. SCOTT. Thank you. Mr. Chairman, I'd like to follow up on, I guess it was your first question because, the operative language in the bill at the top of page 2 says, "Whoever knowingly modifies caller ID information with intent to mislead the recipient of the call as to the identity of the person making the call shall be fined, imprisoned" and so forth. So the intent is to mislead.

What we have heard is we're not trying to cover those who mislead for innocent purposes. So under the exceptions, if we have any blocking of the caller ID, the person looking at the caller ID knows it's been blocked, so you're getting no information, rather than false information. And the second exception is law enforcement activities.

So, Representative Murphy, I assume that you would want us to make it clear that this is not aimed at innocent misinformation?

Mr. MURPHY. Yes. That's why I look to the wisdom of the Committee on this, and it would be very helpful to do that; although I recognize that that is a—intent, as a very important example the Chairman used, would be a good one. On the other hand, if someone used a phoney caller ID to get you out of the house so they could come steal your truck, then it becomes that second level.

Mr. SCOTT. We are not suggesting that the service should not be available at all; is that right?

Mr. MURPHY. That's not what I'm suggesting either, because what happens is—for example, if you were making a call out of your office in the House of Representatives from your private line on your desk, that number does not show up on the receiver, so it's not a matter of trying to prevent that from being done at all but its being done in misleading circumstances.

Mr. SCOTT. In fact, a caller ID number is displayed. It's just the number for the switchboard, not—or some other number that you can't get through.

Mr. MURPHY. That's correct.

Mr. SCOTT. A number is displayed——

Mr. MURPHY. Yes.

Mr. SCOTT.—showing what looks like a congressional office. It's just not your number.

Mr. MURPHY. It's the same thing. Many businesses use that so that the individual's private line on their desk is not accessible for people to call.

Mr. SCOTT. And sometimes you would want displayed a better number to call back, so it is a friendly——

Mr. MURPHY. Correct.

Mr. SCOTT. If you've got five lines in your office and you pick up one line, and if they call back, you'd like them to call the first line, you're not aiming at that.

Mr. MURPHY. Not at all.

Mr. SCOTT. So the service should be available, just not for criminal activities.

Under the exceptions, Mr. Sabin, you have law enforcement exceptions. Are there other—should there be other exceptions? I know women's shelters have an interest in keeping the phone number secret. Are there ways of getting other exceptions in here?

Mr. SABIN. We're open to working with the Committee to establish appropriate exceptions. The two that are articulated in the draft bill, we believe, are proper, and we would support both the law enforcement exception for law enforcement intelligence purposes as well as the call blocking. As to your prior——

Mr. SCOTT. The call blocking is not an issue because that's not false information.

Mr. SABIN. Correct.

Mr. SCOTT. The person knows they're not getting the information, so that—and that's—I think we've covered that——

Mr. SABIN. Okay.

Mr. SCOTT.—but could there be other legitimate purposes for misinformation? I think the women's shelters all have caller ID blocked.

Mr. SABIN. Right. So you could have certain means by which the person who is making—receiving the call could have the call-blocking mechanism instituted so you could have that kind of protection.

Mr. SCOTT. I mean the outgoing calls from a women's shelter——

Mr. SABIN. Okay. So then you could have that means as well.

Mr. SCOTT.—would have, I think, blocked information. Would they be—would you want them to have the option of having another callback number, misinformation?

Mr. SABIN. See, that goes to the range of choices and the preferences of what number you would want to have the—receiving for the number; so you could work through certain circumstances involving that, but that just is a restriction of choice in that regard.

Mr. SCOTT. Okay. Mr. Chairman, if there's going to be another round, I just have another series, and I'll just begin the next series.

Mr. COBLE. Yes, we'll have a second round.

The distinguished gentleman from Florida, Mr. Keller.

Mr. KELLER. Thank you, Mr. Chairman, and let me begin with my colleague, Mr. Murphy.

Is there currently any criminal statute that specifically prohibits spoofing?

Mr. MURPHY. Not that I'm aware of. In fact, the Web sites for these specifically say it is legal to do this.

Mr. KELLER. Okay. Mr. Sabin, let me put that to you.

There is no specific, at least Federal statute, in the area of spoofing?

Mr. SABIN. Correct. There is no specific Federal statute. We rely upon other statutes to address the fraud under Title 18 as well as, for example, unlawful access to computer systems without authority. Under Title 18, United States Code, section 1030, 2701, relating to unopened voice mail is another provision. So there are cer-

tain provisions that we can sort of "ad hoc" approach, but in terms of clarity and specificity, we support the implementation of a specific bill targeting spoofing.

Mr. KELLER. So if you had like a crystal-clear case brought to you by some law enforcement agency and asked DOJ to prosecute it, you would have to use some more generic, general fraud statute or refer it to, like, the State to see if there's any State statute on point?

Mr. SABIN. I'm not aware of any States. I had some discussion with folks. I believe there's a bill pending in Alaska, and maybe one in Florida, on the State level.

What we have seen is the concept of SWATing where there's a number of incidents where—hostage pranks or representations that hostage-taking or bomb incidents are occurring, and you have SWAT teams respond to a particular location. And that kind of hoax is obviously a drain on law enforcement resources and of concern to the individuals whose homes are surrounded by SWAT teams. So that's another kind of Federal offense or incidence of factual circumstances that we've seen.

Mr. KELLER. Before I move on to Mr. Murphy, let me say I noticed in the penalties here it has a fine or a penalty of up to 5 years. And there's no mandatory minimums—which I've been around Chairman-Elect Scott for a long time now, for 6 years—I would think because it doesn't have the mandatory minimum, that would make it easier for him to swallow. I will yield him time to respond to that.

Mr. SCOTT. I think the gentleman knows me well.

Mr. KELLER. Okay. So that's good. You've drafted it well, and hopefully we'll be able to move this at some point for you.

Mr. Kiko, as the chief of staff of the Judiciary Committee, you were a victim of this, I see, so they have really spoofed the wrong person here.

Mr. KIKO. Yeah, I think they have.

Mr. KELLER. I think I may be a victim of spoofing, too. I keep getting calls from this organization called Jenny Craig, and I can't imagine why they'd be calling me, but——

Mr. MURPHY. I might add, on Mr. Kiko's calls, I believe he began to get those calls after we introduced our bill. There is no link between that in order to help him to move this bill.

Mr. KELLER. Okay. Mr. Martin, have you heard from members of your organization who have fallen victim to this scheme as well?

Mr. MARTIN. Mr. Keller, not many as I said in my testimony, but it is a growing problem. It is on the horizon. We're aware of that, and we really are appreciative that this Committee is moving ahead and being proactive on this issue.

Mr. KELLER. Well, I want to just conclude by commending Congressman Murphy for drafting this legislation. I think it's not only a worthy issue, but you've drafted it in a nice, narrow way that I think should ultimately enjoy bipartisan support, and I appreciate all of your time and effort in this.

And, Mr. Chairman, I'll yield back.

Mr. COBLE. I thank the gentleman from Florida, and since there are only three of us here, we will have a brief second round.

Mr. Murphy and/or Mr. Sabin, distinguish between your bill, Mr. Murphy, and the House-passed Truth in Caller ID Act.

Mr. MURPHY. Well, sir, in the previous bill, the Truth in Caller ID Act, asked the FCC to create a rule to make caller ID fraud illegal after 6 months within enactment. It has no penalties with it. I don't think it provides any of the distinctions. It is truly left up to the FCC to provide the definitions. And the problem is that if one continues—if one gets the equipment and can develop this on their own at home, just because it's illegal you may shut down Web sites, but you don't stop individuals from using that, especially if there is no penalty involved with that. And I think that at the level this is and how it can be used nationally for major crimes, it is important that we actually put some teeth behind this and some penalties.

Mr. COBLE. Do you concur, Mr. Sabin?

Mr. SABIN. I do. I agree in terms of the law enforcement objective. And I also believe it addresses, if I'm not mistaken, not only land line cell phones but Voiceover Internet Protocol, which I'm not sure was in the other bill.

Mr. COBLE. Well, now that I have you in my sights, Mr. Sabin, I'll come back with a second question.

Mr. SABIN. My pleasure.

Mr. COBLE. You testified that terrorists, kidnappers and other criminals oftentimes use caller ID spoofing to mislead law enforcement or to throw them off the trail of their criminal investigations.

Do you know of any cases in which this has actually happened?

Mr. SABIN. My point was relating to SWATing, the idea that you have a dire emergency situation. And we have, in talking to the investigative authorities, 30 to 40 incidents that have occurred nationwide where you have SWAT team responses to a particular location where caller ID spoofing had caused that kind of response to be one that drains time, energy and resources as well as to, obviously, the victims at the particular location. So, yes, it has obviously the potential, as other panelists have mentioned, but those are grounded in specific incidents of SWATing responses.

Mr. COBLE. Thank you, sir. Mr. Murphy.

Mr. MURPHY. Mr. Chairman, if I can add to that, some of the risk, too, is that not only do these services change your phone number, they'll also offer to disguise your voice. They'll change a male to a female voice and a female to a male voice, which actually adds to some of the risk and prevents law enforcement from finding out. They cannot do a quick star 69 or star 57 to trace the call and find out where this is really coming from.

It really in many cases—I believe it may even require a subpoena to track that down. And if they don't even know what the voice is, that adds to the risk.

One of the things I worry about with the SWAT instances, imagine some poor fellow who walks out of his house, who maybe is about to go hunting, only to see a number of people there with their guns up at him. Luckily, no one has been harmed under these circumstances yet, but I think it is a very dangerous situation.

Mr. COBLE. Thank you. I have about 2 minutes to go.

Mr. Martin, do you or Mr. Kiko want to add anything? I have no further questions.

Mr. MARTIN. No.

Mr. KIKO. No, sir.

Mr. COBLE. The distinguished gentleman from Virginia.

Mr. SCOTT. Thank you, Mr. Chairman. I just have one or two questions.

First, Mr. Sabin, you mentioned civil as well as criminal sanctions. By "civil sanctions," did you mean the Department of Justice bringing a civil action; or did you mean a private cause of action against the spoofer, which I think would probably go without saying? I mean it's—certainly, you could find that under the previous tort system.

Would there be a specific right of action, or are you talking about DOJ action?

Mr. SABIN. DOJ, potentially injunctive relief, potentially other kinds of civil remedies for a particular tort or the like.

Mr. SCOTT. And would there be any difficulty in the victim having a civil—a private right of action?

Mr. SABIN. I don't think we would be opposed to that. I haven't really thought through that aspect, but I believe that that would be appropriate to pursue by the particular victim through their own lawyer and bringing of that suit.

Mr. SCOTT. But you wouldn't be—and do you think we would need to specifically put that in the bill, that there is a right of action; or do you think there's just inherently a right of action when you have committed—when you have victimized somebody like this, that there is just an inherent right of action?

Mr. SABIN. I would think we would want—I would want to talk to the subject matter experts on that, but I think that that would be a particular cause of action in some kind of civil tort that would be available.

Mr. SCOTT. Already, under present law.

Mr. SABIN. Yeah, I believe that's accurate, but I can check with the Subcommittee on that.

Mr. SCOTT. Thank you. And also on the sentencing, since we have a Sentencing Commission, would not the Sentencing Commission establish guidelines for the appropriate sentence based on the level of harassment, the level of fraud, the amount of money involved in the fraud, and the number of people victimized? Would the Sentencing Commission be able to deal with that appropriately within the bill?

Mr. SABIN. Yes. You would have the Sentencing Commission apply those and other factors to provide uniformity throughout the Nation on a sentencing basis.

Our suggestion was that, based upon the means by which this was used to facilitate another crime and the egregiousness of that crime, you could have a statutory maximum that would, like in Title 18, I believe, either 1028 or 1030, have a graduated series of penalties as a statutory basis of 5 years or 10 years, or even as to a misdemeanor level to provide the full breadth of prosecutorial options.

Mr. SCOTT. Thank you, Mr. Chairman.

Mr. COBLE. Thank you, Mr. Scott.

Before we adjourn, Mr. Kiko, speaking for Mr. Scott and the entire membership of this Subcommittee, we thank you for your

many years of service on the Hill, and we thank the other three witnesses for your time and your testimony today.

In order to ensure a full record of the adequate consideration of this important issue, the record will be left open for additional submission for 7 days. Also, any written questions that a Member wants to submit should be submitted within this same 7-day period.

This concludes the legislative hearing on the Preventing Harassment through Outbound Number Enforcement Act. Thank you for your cooperation, and the Subcommittee stands adjourned.

[Whereupon, at 10:54 a.m., the Subcommittee was adjourned.]