HB

308

SENATE COMMITTEE REPORT

DATE: 4/19/06

FURTHER: Finance

DATE TURNED
IN TO OFFICE:_____

Judiciary Committee considered CS FOR HOUSE BILL NO. 308(JUD) am

HB 308 CALLER ID HACKERS

"An Act relating to false caller identification."

and recommends:

[ ] be **replaced** with _____ **CS** _____ (_____)

[ ] adopt **previous** _____ **CS** _____ (_____)

[ ] attached amendment(s)

[ ] adopt Letter of Intent by _____ Committee

[ ] further referral to _____ Committee

CS Senate Bill:
[ ] Same Title
[ ] New Title

SCS House Bill:
[ ] Same Title
[ ] Technical Title Change
[ ] New Title w/ SCR #____

NEW FISCAL NOTE(S):

Department	Date	Fiscal	Indet.	Zero	FN#

PREVIOUS FISCAL NOTE(S):

Department	Date	Fiscal	Indet.	Zero	FN#

[ ] **APPROPRIATION - no fiscal note**

SIGNATURES AND RECOMMENDATIONS:	DO PASS	DO NOT PASS	NO REC	AMEND
	X			
	X			
	X			
	X			
CHAIR:	✓			

Alaska State Legislature

Chairman
Military & Veterans' Affairs Committee

Member
Labor and Commerce Committee
State Affairs Committee
Economic Development, Trade & Tourism Committee
Education Committee
Joint Armed Services Committee

Finance Subcommittees
Labor & Workforce Development
Community & Economic Development
Military & Veterans' Affairs

A Communication From
REPRESENTATIVE BOB LYNN
District 31 Anchorage

E-Mail: Representative_Bob_Lynn@legis.state.ak.us
"Bob Lynn's Alaska Blog" AlaskaDistrict31.blogspot.com

Session:
Alaska State Capitol
Juneau, AK 99801-1182

Phone: (907) 465-4931
Fax: (907) 465-4316
Toll Free: (800) 870-4391

Interim:
716 W. 4th Ave., #650
Anchorage, AK 99501-2133

Phone: (907) 269-0205
Fax: (907) 269-0207

SPONSOR STATEMENT

CSHB308

An Act relating to false caller identification

Warning: Do not trust your telephone caller ID. The name and number you see may be false. Both private individuals and commercial spoofers can now cause false caller identification to be displayed on your caller ID screen. False caller identification is more than pranks, or annoyance. The power to create serious mischief with Caller ID spoofing technology is almost unlimited and it can facilitate fraud, and can be potentially dangerous.

For example, some financial institutions use caller ID to authenticate telephone requests for personal account information. With a few personal tidbits and your spoofed number, an impostor could access your bank or credit card account. Scam artists who appear to be phoning from a reputable agency can defraud their victims with ease. There's potential for hoax emergency calls with false caller ID to law enforcement or the fire department. Predators could use caller ID spoofing to commit crime against women and children.

Anyone with sufficient computer and telephonic skills can spoof telephone caller Identification systems. In fact an entire telephone spoofing industry has emerged, and is growing daily. With one service for the price of a ten-dollar calling card anyone can change what someone sees on their caller ID display and even change their voice. These spoofing services can work with mobile phones, landlines as well as telephone services that are routed via the Internet.

CSHB308 is a simple measure, that doesn't get into the technological complexities of how the spoofing gets to the display on your Caller ID. If you insert false Caller ID information into a Caller ID system a crime has been committed.

Alaska should take whatever action possible within its jurisdiction to stem the abuse of "Caller ID Spoofing." CSHB-308 will make it class B misdemeanor for any person who inserts false information into a Caller ID system, except for legitimate law enforcement, intelligence or security agencies.

24-LS0779\F
Bannister
1/25/06

CS FOR HOUSE BILL NO. 308( )

IN THE LEGISLATURE OF THE STATE OF ALASKA

TWENTY-FOURTH LEGISLATURE - SECOND SESSION

BY

Offered:
Referred:

Sponsor(s): REPRESENTATIVES LYNN, Dahlstrom, Wilson, Gatto, Neuman, Kerttula, Chenault, Anderson, Gardner, LeDoux, Olson, Croft, Elkins, McGuire

A BILL

FOR AN ACT ENTITLED

"An Act relating to false caller identification."

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF ALASKA:

* **Section 1.** AS 45.45 is amended by adding a new section to read:

Sec. 45.45.940. False caller identification. (a) A person may not knowingly insert false information into a caller identification system.

(b) This section does not apply to law enforcement agencies of the federal government, the state government, or a municipality.

(c) A person who knowingly inserts false information into a caller identification system is guilty of a class B misdemeanor.

(d) In this section,

(1) "caller" means a person who places a call by a telephone or over a telephone line, even if the person begins the call on a computer;

(2) "caller identification system" means a listing of a caller's name, telephone number, or name and telephone number that is shown to a recipient of a call when the recipient answers;

(3) "insert" means insert by voice communication, by written communication, or by typing into a computer;

(4) "knowingly" has the meaning given in AS 11.81.900.

* **Sec. 2.** AS 45.50.471(b) is amended by adding a new paragraph to read:

(51) violating AS 45.45.940 (false caller identification).

FISCAL NOTE

STATE OF ALASKA
2006 LEGISLATIVE SESSION

Fiscal Note Number: 1
Bill Version: CSHB 308(JUD)
(H) Publish Date: 3/30/06

Revision Date/Time (Note if correction): 3/21/06 9:06 a.m.
Dept. Affected: Administration
Title: An Act relating to false caller identification
RDU: Legal and Advocacy Services
Component: Public Defender Agency
Sponsor: Rep. Lynn
Requester: (H) JUD
Component No.: 1631

Expenditures/Revenues (Thousands of Dollars)

Note: Amounts do not include inflation unless otherwise noted below

OPERATING EXPENDITURES	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012
Personal Services	0.0	0.0	0.0	0.0	0.0	0.0
Travel						
Contractual						
Supplies						
Equipment						
Land & Structures						
Grants & Claims						
Miscellaneous						
TOTAL OPERATING	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**
CAPITAL EXPENDITURES						
CHANGE IN REVENUES ( )						

FUND SOURCE (Thousands of Dollars)

1002 Federal Receipts						
1003 GF Match						
1004 GF	0.0	0.0	0.0	0.0	0.0	0.0
1005 GF/Program Receipts						
1037 GF/Mental Health						
Other (Specify Type--Do not abbreviate)						
TOTAL	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**

Estimate of any current year (FY2006) cost: 0.0
Mark this box (X) if funding for this bill is included in the Governor's FY 2007 budget proposal:

POSITIONS

Full-time						
Part-time						
Temporary						

ANALYSIS: *(Attach a separate page if necessary)*

This legislation would create the new crime of False Caller Identification for inserting false information into a caller identification system. False Caller Identification would be a class B misdemeanor.

This legislation is not expected to have a fiscal impact on the Public Defender Agency.

Prepared by: Quinlan Steiner, Director — Phone: (907) 334-4414
Division: Public Defender Agency — Date/Time: 3/21/06 9:06 a.m.
Approved by: Mike Tibbles, Deputy Commissioner — Date: 3/21/2006
Agency: Administration

(Revised 9/7/2005 OMB)

FISCAL NOTE

STATE OF ALASKA
2006 LEGISLATIVE SESSION

Fiscal Note Number: 2
Bill Version: CSHB 308(JUD)
(H) Publish Date: 3/30/06

Revision Date/Time (Note if correction):
Dept. Affected:
Title: Caller ID Hackers
RDU: Alaska Court System
Component: Trial Courts
Sponsor: Representative Lynn
Requester:
Component No:

Expenditures/Revenues (Thousands of Dollars)

Note: Amounts do not include inflation unless otherwise noted below.

OPERATING EXPENDITURES	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012
Personal Services						
Travel						
Contractual						
Supplies						
Equipment						
Land & Structures						
Grants & Claims						
Miscellaneous						
TOTAL OPERATING	0.0	0.0	0.0	0.0	0.0	0.0
CAPITAL EXPENDITURES						
CHANGE IN REVENUES ( )						

FUND SOURCE (Thousands of Dollars)

1002 Federal Receipts						
1003 GF Match						
1004 GF						
1005 GF/Program Receipts						
1037 GF/Mental Health						
Other (Specify Type--Do not abbreviate)						
TOTAL	0.0	0.0	0.0	0.0	0.0	0.0

Estimate of any current year (FY2006) cost: 0.0
Mark this box (X) if funding for this bill is included in the Governor's FY 2007 budget proposal:

POSITIONS

Full-time						
Part-time						
Temporary						

ANALYSIS: *(Attach a separate page if necessary)*

The court system does not anticipate any fiscal impact from the passage of HB 308

Prepared by: Doug Wooliver, Administrative Attorney — Phone: 463-4750
Division: Alaska Court System — Date/Time: 3/17/06 @ 10:30 am
Approved by: Doug Wooliver for Stephanie Cole, Adminstrative Director — Date: 3/17/2006
Agency: Alaska Court System

(Revised 9/7/2005 OMB)

FISCAL NOTE

STATE OF ALASKA
2006 LEGISLATIVE SESSION

Fiscal Note Number: 3
Bill Version: CSHB 308(JUD)
(H) Publish Date: 3/30/06

Revision Date/Time (Note if correction):
Dept. Affected: Public Safety
Title: "An Act relating to false caller identification "
RDU: Alaska State Troopers
Component: AST Detachments
Sponsor: Representative Lynn
Requester: House Judiciary Committee
Component No: 2325

Expenditures/Revenues (Thousands of Dollars)

Note: Amounts do not include inflation unless otherwise noted below.

OPERATING EXPENDITURES	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012
Personal Services						
Travel						
Contractual						
Supplies						
Equipment						
Land & Structures						
Grants & Claims						
Miscellaneous						
TOTAL OPERATING	0.0	0.0	0.0	0.0	0.0	0.0
CAPITAL EXPENDITURES						
CHANGE IN REVENUES ( )						

FUND SOURCE (Thousands of Dollars)

1002 Federal Receipts						
1003 GF Match						
1004 GF						
1005 GF/Program Receipts						
1037 GF/Mental Health						
Other (Specify Type--Do not abbreviate)						
TOTAL	0.0	0.0	0.0	0.0	0.0	0.0

Estimate of any current year (FY2006) cost: 0.0
Mark this box (X) if funding for this bill is included in the Governor's FY 2006 budget proposal:

POSITIONS

Full-time						
Part-time						
Temporary						

ANALYSIS: *(Attach a separate page if necessary)*

This proposed legislation will have no fiscal impact on the Department of Public Safety

Prepared by: Lieutenant James Helgoe
Phone: 907-269-4532
Division: Alaska State Troopers
Date/Time: 3/17/06 1:54 PM
Approved by: Commissioner William Tandeske
Date: 3/17/2006
Agency: Department of Public Safety

(Revised 9/23/2004 OMB)

Alaska State Legislature

Chairman
Military & Veterans' Affairs Committee

Member
Labor and Commerce Committee
State Affairs Committee
Economic Development, Trade & Tourism Committee
Education Committee
Joint Armed Services Committee

Finance Subcommittees
Labor & Workforce Development
Community & Economic Development
Military & Veterans' Affairs

A Communication From
REPRESENTATIVE BOB LYNN
District 31 Anchorage

E-Mail: Representative_Bob_Lynn@legis.state.ak.us
"Bob Lynn's Alaska Blog" AlaskaDistrict31.blogspot.com

Session:
Alaska State Capitol
Juneau, AK 99801-1182

Phone: (907) 465-4931
Fax: (907) 465-4316
Toll Free: (800) 870-4391

Interim:
716 W. 4th Ave., #650
Anchorage, AK 99501-2133

Phone: (907) 269-0205
Fax: (907) 269-0207

Sectional Analysis for CSHB 308 (JUD): "Caller ID spoofing,"
An Act relating to false caller identification.
Released: March 31, 2006
Dirk Moffatt, staff for Rep. Bob Lynn

Section 1. Adds a new section, AS 45.45.940, creating the crime of false caller identification for a person who knowingly inserts false information into a caller identification system. The crime would be a class B misdemeanor.

Section 2. Amends AS 45.50.471 to add the new violation of false caller identification to the list of unlawful acts and practices under this section.

Alaska State Legislature

Chairman
Military & Veterans' Affairs Committee

Member
Labor and Commerce Committee
State Affairs Committee
Economic Development, Trade & Tourism Committee
Education Committee
Joint Armed Services Committee

Finance Subcommittees
Labor & Workforce Development
Community & Economic Development
Military & Veterans' Affairs

A Communication From
REPRESENTATIVE BOB LYNN
District 31 Anchorage

E-Mail: Representative_Bob_Lynn@legis.state.ak.us
"Bob Lynn's Alaska Blog" AlaskaDistrict31.blogspot.com

Session:
Alaska State Capitol
Juneau, AK 99801-1182

Phone: (907) 465-4931
Fax: (907) 465-4316
Toll Free: (800) 870-4391

Interim:
716 W. 4th Ave., #650
Anchorage, AK 99501-2133

Phone: (907) 269-0205
Fax: (907) 269-0207

Changes from the original version of HB308 to CSHB 308 (JUD):
"Caller ID spoofing"
Released: April 19, 2006

On March 29, 2006, the House Judiciary Committee passed a committee substitute to HB308 by adding page 1, lines 6 through 9 of CSHB 308 (JUD):

(b) This section does not apply to
(1) law enforcement agencies of the federal government, the state government, or a municipality; or
(2) intelligence or security agencies of the federal government.

On March 18, 2006 the State House Passed CSHB 308 (JUD) with the following technical amendment on page 2, line 4 by Deleting the word "typing" and inserting the phrase "otherwise entering it" of CSHB 308 (JUD) AM.

Technology facilitates Caller ID spoofing

AP Associated Press

Rep. Tim Murphy, R-Penn., picks up his telephone handset in his office in the Cannon House Office building on Capital Hill, Wednesday, March 1, 2006 in Washington. Last fall, Murphy's office started getting phone calls from constituents who complained about receiving recorded phone messages that bad-mouthed Murphy. The constituents were especially upset that the messages appeared to come from the congressman's own office. At least, that's what Caller ID said. In the last few years, Caller ID spoofing has become much easier. Millions of people have Internet telephone equipment that can be set to make any number appear on a Caller ID system. (AP Photo/Pablo Martinez Monsivais)

By Peter Svensson, AP Technology Writer | March 1, 2006

NEW YORK --Last fall, U.S. Rep. Tim Murphy's office started getting phone calls from constituents who complained about receiving recorded phone messages that bad-mouthed Murphy.

The constituents were especially upset that the messages appeared to come from the congressman's own office. At least, that's what Caller ID said.

"People thought we were making the calls," Murphy said.

The calls, which the Pennsylvania Republican estimated in the thousands, were apparently placed with fake Caller ID. That has been possible for a long time, but it generally required special hardware and technical savvy.

In the last few years, Caller ID spoofing has become much easier. Millions of people have Internet telephone equipment that can be set

ARTICLE TOOLS

PRINTER FRIENDLY
SINGLE PAGE
E-MAIL TO A FRIEND
TECHNOLOGY RSS FEED
MOST E-MAILED

MORE:
Business section
Latest business news

GO

to make any number appear on a Caller ID system. And several Web sites have sprung up to provide Caller ID spoofing services, eliminating the need for any special hardware.

For instance, Spoofcard.com sells a virtual "calling card" for $10 that provides 60 minutes of talk time. The user dials a toll-free number, then keys in the destination number and the Caller ID number to display. The service also provides optional voice scrambling, to make the caller sound like someone of the opposite sex.

Caller ID spoofing appears to be legal, though many of its uses are not. The Federal Communications Commission has never investigated the issue, spokeswoman Rosemary Kimball said.

Lance James, chief scientist at security company Secure Science Corp., said Caller ID spoofing Web sites are used by people who buy stolen credit card numbers. They will call a service such as Western Union, setting Caller ID to appear to originate from the card holder's home, and use the credit card number to order cash transfers that they then pick up.

Exposing a similar vulnerability, Caller ID is used by credit-card companies to authenticate newly issued cards. The recipients are generally asked to call from their home phones to activate their cards. Some card companies maintain, however, that they use additional means to confirm new cards. And caller ID spoofing may not work for calls to 1-800 numbers, where the hardware can identify calls using a separate technology.

Two spoofing services contacted by The Associated Press, Spoofcard.com and Telespoof.com, did not return messages seeking comment about their business. However, some of the five or so Web sites in the business don't appear to be completely unscrupulous. James said he had been hired by a few of them, which he would not name, to help stop the Western Union scam.

Also, both Spoofcard.com and SpoofTel.com say they will surrender call logs to authorities in response to subpoenas. Spoofcard.com's site says the service is "intended for entertainment purposes only."

Telephone companies can trace calls to their origin regardless of the Caller ID information they carry, but the process is laborious, especially since a call may be carried by several companies before reaching its destination. The fragmented nature of the telephone network also makes it technically difficult for the carriers to prevent spoofing.

At Verizon Communications Inc., security manager John Lewandowski said the company often gets complaints about fake Caller ID after a telemarketer has spoofed his number to cover his tracks.

In a typical case, someone will be jarred in the middle of the night by repeated telemarketing calls. He checks Caller ID, calls the number -- which is false -- and starts "cussing out" the person at the other end of the line, Lewandowski said.

"And that poor guy was asleep. It wasn't him at all," Lewandowski said. The company investigates and tracks down the callers, he added.

Apart from fraud and telemarketing, Caller ID spoofing can be used

LATEST TECHNOLOGY NEWS

- EU leaders call for lower roaming charges
- Nintendo urges game makers to innovate
- Cablevision gets Mets back in SportsNet deal
- Extra costs a worry for next-gen DVD adoption
- Toshiba wins flash memory patent suit vs Hynix
- More technology news

BOSTON.COM'S MOST E-MAILED

- A generous Bush always thinking of others
- Bush shuns Patriot Act requirement
- The obligation of unwanted fatherhood
- Hundreds of teachers not qualified, city says
- 'The Simpsons' to show live-action opening
- See full list of most e-mailed

SEARCH THE ARCHIVES

GO

- Advanced search / Historic Archives

for pranks and spying.

In one case, SWAT teams surrounded a building in New Brunswick, N.J., last year after police received a call from a woman who said she was being held hostage in an apartment. Caller ID was spoofed to appear to come from the apartment.

It's also easy to break into a cell phone voice mailbox using spoofing, because many systems are set to automatically grant entry to calls from the owner of the account. Stopping that requires setting a PIN code or password for the mailbox.

In a slightly more complicated fashion, spoofing was part of the technique used by a hacker who broke into Paris Hilton's cell-phone voicemail in 2004, according to security consultant Kevin Mitnick, who said he was citing hacking sources. The hacker apparently called the celebrity socialite posing as a technical-support person from the carrier, and lured the password from her.

That is known as a "pretext" call -- someone poses on the phone as a customer, employee or even a regulator to obtain personal information from companies and individuals. And indeed, while Spoofcard.com contends that its service is for "entertainment purposes," it also notes that "Private Investigators will find Caller ID spoofing valuable for pretext calls."

Robert Douglas, a privacy consultant in Colorado, testified before Congress last month that pretexters trade tips on finding the best spoofing services.

Pretexters generally claim their practices are legal, as long as they don't involve financial information. A bill introduced in the Senate would make it illegal to pose as someone else to obtain phone records, or to buy records from phone company insiders.

Douglas would like legislation against Caller ID spoofing as well, but there appears to be little interest in Washington.

"If I'm paying extra for Caller ID, which I do ... there should be some ability on my part to believe what I'm getting," Douglas said.

In Alaska, State Representative Bob Lynn has introduced a bill to make spoofing a misdemeanor. "False caller identification is more serious than pranks, or the annoyance of intrusive telemarketing," Lynn writes. "It facilitates fraud, and can be potentially deadly."

However, it is unclear what effect the bill would have. As Lynn notes, Caller ID is a federal issue. ■

MORE:
Business section | Latest business news | Globe front page | Boston.com

SIGN UP FOR: Globe Headlines e-mail | Breaking News Alerts

PRINTER FRIENDLY | SINGLE PAGE | E-MAIL TO A FRIEND | AVAILABLE RSS FEEDS | MOST E-MAILED

It's not clear if Murphy's criticism figured in Barton's introduction of a new FCC-focused bill explicitly outlawing spoofing; Murphy couldn't be reached for comment. Engel is the Barton bill's lead Democratic sponsor. A cosponsor of the original bill with Engel, Rep. Wilson (R-N.M.), isn't listed as a Barton bill cosponsor; her office couldn't be reached for comment. Barton's spokesman said that for "some reasons of technicality, [spoofing] really needs to be addressed by the FCC" instead of the FTC.

The FCC is a better agency to handle spoofing rules, Electronic Privacy Information Center Dir.-West Coast Chris Hoofnagle told us. With FTC jurisdiction, "it would have suffered from all sorts of blind spots -- common carriers... are generally exempt from FTC rules," Hoofnagle said. But the Barton bill's lack of an intent requirement "will create major problems for many," he said: "Many businesses and government do not transmit their direct line -- they 'spoof' the institutional number. Are they on the hook under this law?" The bill should make clear that intent to deceive is the clincher, Hoofnagle said. -- ***Greg Piper***

'Percolates Up'

WildBlue Jumps Digital Gap without U.S. Funds; State Interest Up

GREENWOOD VILLAGE, Colo. -- Since setting up its first customer in Strasburg, Colo. nearly a year ago, NRTC-backed satellite broadband provider WildBlue has been bridging the digital divide in rural communities across the U.S. without govt. aid. The firm's main market lies beyond the reach of terrestrial broadband -- particularly in farming and ranching communities targeted by WildBlue advertising the past year in agriculture magazines and local radio spots.

WildBlue's service might seem a natural means of meeting the President's broadband pledge and FCC rural connectivity goals. But the firm doesn't qualify for federal USDA grants, and state support has been stirred only by word of mouth, WildBlue Sr. Vp & Gen. Counsel David Brown told us in an interview. Faster than dial-up but slower than wired options, the least expensive WildBlue access is $49.95 a month.

The U.S. has about $2 billion in USDA Rural Utilities Services loans to spend on rural broadband deployment through 2007 (CD Sept 20 p6). Satellite broadband is touted as an ideal rural broadband solution, but "it doesn't really fit the rules around the Department of Agriculture money," said Brown. The USDA funds are "really meant for small local telcos as opposed to somebody that can distribute nationally," Brown said.

The USDA rules, written in the early 1990s, "didn't have satellite in mind," Brown said. If a broadband provider can distribute service nationally, including regions already wired with DSL or cable, "then you don't qualify for the money," he said. WildBlue relies on the NRTC for political maneuvering, and the cooperative "has been leading the charge for the USDA RUS rules to be written in a more technologically neutral way," Brown said.

If WildBlue is looking for govt. support in bridging the digital divide, it might have more luck at the state level. Several states are "very interested in the service," thanks to WildBlue's ability to get broadband to rural residents, WildBlue Pres. & COO Kenneth Carroll said: "They're very interested in working with us to develop programs for rural constituents to provide the service where cable, DSL or fixed wireless isn't available."

So far state interest is from the bottom up, he said: "Somebody in the state government got the service, or their parents got the service out on their farm or ranch, and it percolates up. Then the state gets interested and says they're going to look at using you to complete the blueprint for service to all constituents."

Tribal connectivity should be included in that vision, Carroll said. "It's an important area," but one that WildBlue hasn't "specifically engaged in," he said. NRTC members and retailers WildBlue works with serve tribal lands, he said: "I don't have specifics, but we are very interested in being able to service those communities."

Angelos proposed to merge MASN with Comcast's regional sports network (RSN). "We're prepared to talk about a potential amalgamation of the 2 systems under an appropriate arrangement," said Angelos: "We're prepared to work at it, and come back and report to your committee our progress." Earlier in the hearing, McCollum said Cox would rather carry one RSN. Cohen echoed that sentiment, telling reporters: "Everyone who is in this business realizes that the best result is to have a single sports network in the same market." Several hurdles stand in the way of a deal with Angelos, including price and MASN's ownership structure, he told the panel.

Comcast wouldn't agree to compulsory arbitration, proposed by Committee Chmn. Tom Davis (R-Va.). That tactic helped resolve a similar dispute in N.Y. between Cablevision and the YES Network, said Davis. Cohen balked: "Compulsory arbitration is not something we would be interested in... We have to run our business and we really can't turn it over to a 3rd party." -- ***Josh Wein***

Action Soon After April Break

Barton Bill Would Ban Deceptive Caller ID, Give FCC Jurisdiction

"Spoofing" caller ID information would be outlawed under a bill introduced by House Commerce Committee Chmn. Barton (R-Tex.) Thurs. The bill would give the FCC power to enforce the bill's provisions within 6 months of enactment. Spoofing refers to services, mostly by Web-based firms, that let a user create phony phone numbers or other data displayed by a call recipient's caller ID. Phone numbers for Republican House offices were used on calls criticizing the members to their constituents. The same was also done with Democratic Party office numbers.

Barton is making the issue a high priority, a Commerce Committee spokesman told us: "I understand we're going to get t this in short order" after the Easter recess.

The bill would apply to traditional and VoIP calls in which the caller causes "any caller identification service to transmit misleading or inaccurate caller identification information." There's an exception for law enforcement. Not all VoIP services are covered; the bill defines VoIP service as that provided "for a fee," excluding free services like Skype's PC-to-PC calling and similar services through instant-messaging programs that don't touch the PSTN. But paid VoIP with "capability" to interconnect with the PSTN -- regardless of whether a particular call made through VoIP actually interconnects -- is covered.

The feds aren't the first to study spoofing services. Fla. Attorney Gen. Charlie Crist (R) in March pursued several sites through their hosting service, GoDaddy.com. Crist asked GoDaddy to provide business record data on SpoofCom.com, SpoofTech.com, SpoofTel.com, SpoofCard.com and TrickTel.

Spoofing services emphasize their utility especially for inquiries into illegal activity. As other sites do, SpoofCard.com says its services are aimed at law enforcement, private investigators, lawyers and insurance agents but aren't limited to their use. The website says private investigators will "find spoofing valuable for pretext calls" -- a loaded term given approval of bills criminalizing pretexting -- impersonation of another's identity to acquire personal records -- in the House and Senate Commerce and Judiciary committees (CD March 31 p2, March 9 p2).

Barton's bill follows one introduced a day earlier by Rep. Engel (D-N.Y.), which simply gave the FTC jurisdiction to classify spoofing as an "unfair or deceptive act." Engel's bill didn't mention the FCC. The FTC provision irked Rep. Murphy (R-Pa.), whose office phone number was among those appropriated by a spoofer in calls to constituents that made critical comments, *Wired News* and *National Review* reported. Murphy, who initially worked with Engel on the bill, came to see the FTC enforcement as too weak, investigation too slow, and likely penalties for violation too small.

FTC = Federal Trade Commission.

Archive

<< 2006

Jan Feb Mar

Most Popular News

- Double trouble for IE
- Picture of a hacker
- Third strike for IE
- Patch Tuesday
- Spam tastes better on Friday

For Potential Authors

Want to become one of our authors and see your work published on Viruslist.com? Contact us!

Caller ID faking targeted by FCC

ByKonstantin Kornakov | Mar 07 2006 09:18 GMT | comment

The service is simple – you call from a number, but the person you call sees a totally different number in the Caller ID display. It sounds innocent enough, but this kind of service has caused the US Federal Communications Commission to initiate an investigation. The problem with Caller ID spoofing is that while it can be used to simply play a joke on someone, it can also facilitate fraud and other criminal activities.

The possibility to fake a Caller ID has existed for a long time in telecoms networks. This is largely due to their disjointed nature with many different companies operating different parts of the telephone line. However, the advent of VoIP services has made it increasingly easy to carry out spoofing without specialized technical knowledge or access to dedicated hardware. The problem lies with less than stringent VoIP operators, which allow calls to be placed using almost any anything in terms of data sent as the caller's ID. Hackers have taken advantage of this flaw and have set up several services, which allow users to purchase pre-paid call time. All the user has to do is dial the number he wants to call and the number he wants displayed as his Caller ID.

Private investigators have flocked to this service in droves, since it gives them the opportunity to pose as other people (according to caller ID information) while on the phone. Some services even offer to change a caller's voice over the line and claim that business professionals can make their calls truly anonymous with Caller ID spoofing. Congressman Tim Murphy, who himself fell victim to this technology, recently put forward one example of the potentially dangerous use of Caller ID spoofing. Last year some of his constituents started receiving calls with pre-recorded messages which abused him. However, the caller ID display showed that these calls came from his office. Another use of this technology involves money-wiring services that use Caller ID for identification purposes, allowing fraudulent money transfers. Fraudsters posing as their victims through the use of this technology have also extracted private consumer information from companies.

It seems that the criminal use of this technology has finally attracted the attention of the authorities. It remains to be seen is whether this will lead to better protection for consumers in the future. Caller ID has proved to be a widely-used service for personal authentication, but has also been shown to be extremely vulnerable and unprotected.

Source:

- MSNBC
- Wired News

Email: webmaster@viruslist.com

REUTERS
KNOW. NOW.

Print this article Close This Window

Scam Artists Dial for Dollars on Internet Phones

Sun Mar 20, 2005 09:40 AM ET

By Andy Sullivan

WASHINGTON (Reuters) - Internet phone services have drawn millions of users looking for rock-bottom rates. Now they're also attracting identity thieves looking to turn stolen credit cards into cash.

Some Internet phone services allow scam artists to make it appear that they are calling from another phone number -- a useful trick that enables them to drain credit accounts and pose as banks or other trusted authorities, online fraud experts say.

"It's like you've handed people an entire phone network," said Lance James, who as chief technology officer of Secure Science Corp. sees such scams on a daily basis.

The emerging scams underline the lower level of security protecting Voice Over Internet Protocol, or VOIP, the Internet-calling standard that has upended the telecommunications industry over the past several years.

Traditional phone networks operate over dedicated equipment that is difficult for outsiders to penetrate. Because VOIP calls travel over the Internet, they cost much less but are vulnerable to the same security problems that plague e-mail and the Web.

Internet worms that snarl online networks can render VOIP lines unusable, and experts at AT&T say VOIP conversations can be monitored or altered by outsiders.

Federal Trade Commission Chairman Deborah Platt Majoras recently warned that unscrupulous telemarketers could use VOIP to blast huge numbers of voice messages to consumers, a technique known as SPIT, for "spam over Internet telephony."

All of these threats remain largely in the realm of theory. Caller ID spoofing, on the other hand, has emerged over the past six months as a useful tool for identity thieves and other scam artists, according to fraud experts.

PRESIDENT BUSH ON THE LINE

Any reporter would scramble for a ringing phone that reads "White House media line" on its caller ID display.

But it's not the Bush administration on the line -- it's security instructor Ralph Echemendia, calling from a mobile phone on a remote Georgia highway.

"You can see how this sort of thing could be used in a very malicious way," said Echemendia, a security instructor at the Intense School, a technology training company.

Caller ID spoofing is not prohibited by law, but the Federal Communications Commission requires telemarketers to identify themselves accurately, a spokeswoman said.

Echemendia built his own system to spoof calls, but several free or low-cost services allow even technical novices to falsify caller ID information as well.

Debt collectors and private investigators use Camophone.com's 5-cents-per-call service to trick people into answering the

phone, according to messages posted on a discussion board.

Traveling salesmen say the service comes in handy when they want clients to return calls to the main office, rather than their motel room.

James said criminal uses of caller-ID spoofing have become common over the last six months.

Wire-transfer services like Western Union (FDC.N: Quote, Profile, Research) require customers to call from their home phone when they want to transfer money in an effort to deter fraud -- a barrier easily sidestepped by any identity thief using a caller-ID spoofing service.

Fraud rings can now transfer money directly out of stolen credit-card accounts, rather than buying merchandise and reselling it, he said.

Western Union spokeswoman Danielle Periera said the company has no other way to verify that transfer requests are valid.

"We try hard to stay one step ahead of them and recognize that scam artists are sophisticated and often change their schemes," she said.

Criminals can use caller-ID spoofing to listen to other people's voice mail, James said, especially when those accounts are not protected by passwords.

They also have begun to use the technology to make it appear that they are calling from a bank or other financial institution, said Dave Jevans, who chairs the Anti-Phishing Working Group, a banking-industry task force.

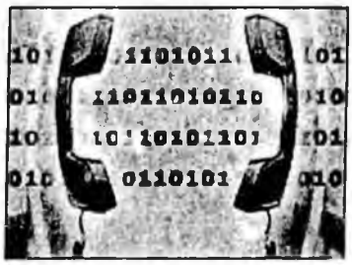
That helps them convince consumers to divulge account numbers, passwords and other sensitive information in a scam that echoes the "phishing" e-mails that have become common, he said.

VOIP industry pioneer Jeff Pulver, whose Free World Dialup service can be used to spoof calls, said he couldn't prevent abuse of his system.

The problem will likely recede as companies like VeriSign Inc. (VRSN.O: Quote, Profile, Research) and NeuStar Inc. develop ways to verify online identities, he said: "We're not there yet, but we're going to get there."

Close This Window

Caller-ID Spoofing: 'Appallingly Bad Idea'



By Erika Morphy
September 2, 2004 1:26PM

A new software system that allows users to fool telephone caller-I opens the door to a variety of abuses. "What an appallingly bad id security firm Sophos.

>> A startup company has developed a software system that allows users to spoof a caller-ID number in order to trick the telephone-call recipient into answering the phone.

Developed by Star38, the service will be marketed solely to collection agencies, private investigators and the police, according to statements made by the company.

The system itself is said to be easy to use, with the user typing in the recipient's number and the number he or she would like to appear on the caller ID.

Appallingly Bad

Critics of the system -- and there are many, even outside the usual privacy/consumer-advocacy brigade -- find the technology frightening. "What an appallingly bad idea," says Graham Cluley, managing consultant for security and antivirus firm Sophos. "It reminds me of the hacker-driven spam and phishing scams that have taken over the Internet," he told NewsFactor.

More on this topic.

In fact, it is a much worse form of deception than Internet fraud, says John Morris, staff counsel for the Center for Democracy & Technology, a Washington-based public-policy organization with a focus on technology.

Reasonable Expectation

"On the Internet, most people understand that the identity of someone who is sending an e-mail may easily be spoofed," Morris told NewsFactor. "But the phone, historically, has had a different set of expectations or assumptions. Most people that have Caller ID assume the number listed is accurate."

In news accounts, Star38 has emphasized its intent to limit the technology to the police, collection agencies and private investigators.

However, "there really isn't anything that will prevent this kind of technology from being used by other firms, such as telemarketers, now that it has been developed," Morris says, adding, "in this age of identity theft, we are skeptical that spoofing other phone numbers on Caller ID is a desirable development."

One scenario, Morris suggests, might be someone purporting to call from a distant relative's house, claiming the person had an accident.

Potential for Abuse

But even assuming that Star38 keeps the technology in the hands of collection agencies, private investigators and the police, there still would be cause for worry.

While the police may well have a legitimate need for the technology in criminal investigations, the potential for abuse by collection agencies and PIs is huge.

For example, there have been cases of stalkers retaining private investigators to find victims who went into hiding

As for collection agencies, the potential for abuse is even wider. "We don't understand what purpose a legitimate collections agency would have in hiding its identity," Morris says.

The typical example, of course, is an agency that uses the system to get a phone-shy debtor to answer the call and coax him or her into paying the debt.

Collection agencies, though, have not entirely shed their less-than-upstanding practices since the passage of the Fair Debt Collection Practices Act. Recently, one firm was fined for continually contacting and harassing a debtor's neighbors -- a

1. Sony Ericsson Intros Bl
2. I.T. Salaries Up the
3. Scientists Find Lost Wo
4. Marketers Bristling at C
5. GM Cuts Dividend, Trim

Most Popular Artic
1. CRM and VoIP: The Be
2. Customers Urge Avoida
3. Another Look at Outsou
4. Pac-West, VeriSign Tea
5. Avaya, Juniper Partner

practice clearly illegal under FDCP.

Over the Line

More often, though, when these agencies go over the line, it is a little more discreet.

Recently, a legal journal reported tnat a court found a collection agency had made false statements as to the time limit of a debt-discount offer; reportedly, the firm told the debtor she had 30 days to make a payment if she wanted to get a percentage taken off her debt. In truth there was no time limit of 30 days -- a deception prohibited by the law.

Which brings us back to Star38's latest contribution to the Internet age. In his first take on the system, Morris says he does not believe the system itself violates the tenets of FDCP. When it gets in the hands of the agencies, though, that may be a different story.

"I do believe we will see some deceptive practices on the part of the agencies that will violate the spirit of FDCP," he says.

Have an informed opinion on this story?
Send a Letter to the Editor.

We want to know what you think.
Send us your Feedback.

Related Topics

- caller-id

Latest News & Special Report

- Convergys Links CRM tc
- Biggest I.T. Outsourcing
- Is On-Demand CRM Rig
- Another Look at Outsour
- VoIP Conversion Gather

AMERICAN PUBLIC MEDIA

Future Tense is an American Public Media program

FUTURE TENSE®
WITH JON GORDON

Search Future T

Subscribe to RSS feed
(What is this?)

Subscribe to Podcast
(What is this?)

E-mail Newsletter
Get *Future Tense* in your inbox each weekday by subscribing to our e-mail newsletter. Technology news, information and interviews at your convenience. Sign up today.

Search Futuretense
go

Future Tense is heard in the United States during broadcasts of the CBC's As It Happens, and in Minnesota on MPR news stations during Morning Edition.

E-mail Future Tense

Broadcast stations

Our Sponsors

March 2005 Archive

March 08, 2005

"Caller ID spoofing" an emerging VoIP security threat

Real Audio | How to Listen

If you have caller ID, you might want to think twice about trusting the information displayed on your telephone. As more people place phone calls over the Internet instead of the wired telephone network, identifying the person on the other end of the line is getting more difficult.

Starting late last summer, people all over the U.S. and Canada got phone calls from a Twin Cities phone number -- a recorded voice offering a deal on wireless phone services. When they called the number to complain, they were patched through to a small Minneapolis company that definitely was not selling Nokias or Blackberries. It was a company that provides janitorial services to area businesses.

Building Resources Corporation office manager Rhiannon Fisk fielded the complaints.

"Around Christmastime, the call volume started to pick up, and we got dozens and dozens every day," she said. " It got to the point where we just had to start ignoring them because it was affecting how we did business."

Understandably, the callers complained angrily about the unwanted telemarketing calls.

"I'll pick up the phone, they immediately say you called my house and I want you to stop calling, and take me off the list, and they usually just hang up," Fisk said.

Fisk sought answers from the company's telephone provider, Integra, but received none. She then complained to the Minnesota Attorney General. The AG's office told fisk that, while nothing could be done, it knew the likely source of the problem: caller ID spoofing. The shady telemarketers, wanting to avoid detection, made it look like it was someone else. It's a mystery why they chose the Minneapolis company.

Scammers have long known how to fake the source of e-mail. Since Voice over IP, or VOIP, sends voices as packets of data, it was perhaps predictable that telephone customers would start seeing a

March 2005

S	M	T	W	Th
		1	2	3
6	7	8	9	10
13	14	15	16	17
20	21	22	23	24
27	28	29	30	31

February 200

S	M	T	W	Th
		1	2	3
6	7	8	9	10
13	14	15	16	17
20	21	22	23	24
27	28			

Archives
March 2005
February 2005
January 2005
December 2004
November 2004
October 2004
September 2004
August 2004
July 2004
June 2004
May 2004
April 2004
March 2004
February 2004
January 2004

Recent Entries
"Caller ID spoofing" emerging VoIP secu threat

problem like e-mail spoofing.

"If you pick up you standard phone today, and you have caller ID, you can see which number is actually calling you, and you have a very high level of assurance that it really is that telephone number," said Stuart McIrvine, security researcher at IBM. Now, when you start to get into Voice over IP, it's very easy for someone to fake that number, so you think the call is coming from somewhere else."

Consumer advocacy groups are just beginning to field complaints about the problem. Jordana Beebe with the Privacy Rights Clearinghouse says she's not sure how many people are being burned by caller ID spofing, but calls it a deceptive practice that should be stopped.

"Caller ID is there so that you know who is calling and you can make a determination about whether you want to take that call or not," she said. "And if for instance that technology is being abused so that you are duped into taking a call that otherwise you wouldn't take, we feel that consumers shouldn't be in that type of situation."

You don't have to be a skilled, devious hacker to trick called ID displays. In the past year, about a half dozen services have cropped up that use VoIP technology to sell caller ID spoofing, at five to ten cents a minute, to consumers. They go by names like "Telespoof," and "Camophone." They're marketed to people who want to hide their true identities, like bill collectors and private investigators. Only one caller ID spoofing service, responded to inquiries from MPR, but the owner wouldn't reveal his name, saying only that he believes his service is ethical and lawful.

Beebe of the Privacy Rights Clearinghouse says new regulations and laws are needed to fight caller ID spoofing. But VoIP is largely unregulated. A spokeswoman at the agency that would most likely have jurisdiction, the Federal Communications Commission, did not respond to numerous requests for comment.

In the meantime, caller ID spoofing could get worse as more consumers and businesses switch to Internet telephone calls.

"What we're going to see is more people devote more time and energy into breaking it, because it's going to become more popular," said David Endler of the Voice Over IP Security Alliance.

Back at the janitorial services firm, office manager Rhiannon Fisk says that mercifully, her phone stopped ringing off the hook about a month ago. The calls ended as mysteriously as they appeared.

Everything Jersey

'Spoofing' lets pranksters dial M for mayhem

Monday, April 11, 2005

BY KEVIN COUGHLIN
Star-Ledger Staff

When a hoax led sharpshooting SWAT teams to shut down a New Brunswick neighborhood last month, the world learned about a dangerous new game called "bombing."

Prank phone calling, once a summer pastime of slap-happy kids, had morphed into a blood sport.

While details still are unfolding on how the New Brunswick emergency call and others like it were faked, experts on privacy and security warn that Internet technology and legal loopholes are handing hoaxsters a powerful weapon to dupe everyone: caller ID "spoofing."

Over the past few months, companies such as Camophone, CovertCall, Telespoof and SpoofTel have sprouted online with offers to place calls that display any callback number you want, for just pennies a minute.

"Be Anyone, Anywhere, Anytime," proclaims the Web site of PI Phone.

PI Phone and rivals Star38 and U.S.Tracers purport to serve only private investigators or law enforcement personnel, who presumably have good reasons for tricking outlaws to answer the phone. But other services welcome all comers; for an extra fee some even will record the results.

"Wanna have some fun? Appear to be someone else, and set up the Ultimate Prank Call," says the Web site for CovertCall, which sponsors a $250 contest for the best prank.

CovertCall suggests fooling debtors into accepting calls, spoofing your business line to keep your personal number private, and exploiting cellular plans that offer free incoming minutes. "Want to chat with sexy singles? Get endless free trials by calling in with random caller IDs!"

On the Web, CovertCall users even debate methods -- and ethics -- of spoofing a spouse's number to access his or her cellular messages.

The Federal Communications Commission and Federal Trade Commission say they have taken no enforcement actions against these services. But others predict it won't be long before an emergency hoax, identity theft or duped domestic violence victim triggers calls for a crackdown.

"The potential for abuse with this technology is huge," says Jordana Beebe of the nonprofit Privacy Rights Clearinghouse, a San Diego group that advocates for consumer privacy protections.

Adds Kevin Mitnick, co-author of "The Art of Intrusion" and a reformed hacker himself: "You can't trust caller ID. There is no assurance that it is coming from the entity that's displaying on the device."

To prove his point, Mitnick used Vonage, the Edison-based Internet phone company, to call a reporter's cell phone. The call appeared to come from the reporter's office number. The ruse took Mitnick only a few seconds.

Many Internet telephone services let users update their accounts with any callback numbers or emergency addresses they choose. This can be a lifesaver. If you're vacationing and making calls over the Internet, you probably want your service provider to direct police to your vacation spot if you punch 911 in an emergency.

(Spoofing 911 calls over conventional phone networks is much harder. They deploy an embedded billing technology, called SS-7, which automatically links a 911 call with the physical address of the telephone. The New Brunswick hoax appears to have been phoned to a regular police line, not to 911.)

Mitnick, who spent almost five years in jail for hacking into companies such as Motorola and Sun Microsystems, says some financial institutions use caller ID to authenticate telephone requests for personal account information. With a few personal tidbits and your spoofed number, he says, an impostor could access your bank or credit card account.

SPOOF WITH EASEActually, spoofing phone calls is nearly as old as caller ID, a service that debuted in New Jersey -- despite protests from privacy advocates -- in the late 1980s. Back then, spoofing required some technical savvy. Now, anyone with a credit card and a phone or online computer can play.

Typically, after setting up an account with a spoofing service, you call its toll-free line or log onto the Web site. Enter a number to call, and the callback number to display, and the service does the rest.

The mere act of faking someone's phone number is not illegal, says Erin McGee of the CTIA, a wireless industry trade association.

Jim Reynolds of Star38 says his company, launched last fall in Delaware by former law enforcement agents for current agents, was the first commercial spoofing service. Other services are copycats and lawbreakers, he says.

"I guarantee those people will be prosecuted. It's only a matter of time," says Reynolds.

Star38 is meant to help the good guys hunt the bad guys; rivals "give people a license to harass people and break the law," he says.

Because Star38's calls are placed entirely over the Internet, they are exempt from FCC regulations, Reynolds contends. Competitors can't make the same claim, he insists.

But most Internet calls hop onto regular phone networks at some point, says Mark Wigfield of the FCC. "We would have to look at the facts" of any case, he says.

Federal Trade Commission rules bar telemarketers from spoofing caller ID to sidestep the national "Do Not Call" registry established in 2003. Some business uses of spoofing also could violate FTC prohibitions against unfair or deceptive trade practices, says spokesman Brad Winter.

Banning all spoofing would be a mistake, says Vonage chief technical officer Louis Mamakos. That might bar legitimate uses for altering callback numbers -- such as directing customers to general help numbers instead of to specific representatives.

In fact, spoofing services actually may help preserve personal privacy, says Jonathan Bick, a

Rutgers University law professor and author of "101 Things You Need to Know About Internet Law." These services restore a right to anonymous speech that caller ID had stripped, Bick says.

"We just have evolving technologies," he says. "And as technologies evolve, so do countermeasures."

THE SPOOFERSThe sudden rise of spoofing services can be tied, variously, to boredom, the National Hockey League, and a struggling college student.

SpoofTel was born in Vancouver two months ago when a computer security specialist named Ryan Purita got bored.

"This is why having no hockey on TV is bad," jokes Purita, referring to the canceled NHL season.

Purita thought the Star38 service sounded cool but was miffed it only served cops. So he cooked up SpoofTel and says it now has about 800 active users who average between 2,000 and 5,000 minutes a day at a dime per minute, Canadian.

He promises to deal swiftly with any reported abuses but defends caller ID spoofing.

"We're offering a service. If someone is using it illegitimately, what can we do? That's the Internet," Purita says.

"They still sell crowbars, don't they? They can be used for many different things. I don't see anybody being stopped from selling guns. I would guess more people are killed by guns than from spoofing caller ID," he says.

Ben Rosenthal also entered the caller ID spoofing business in January, with his PI Phone service for private investigators.

"I saw an opportunity and profit there, and a way to do it honorably and legally, and jumped on it," says Rosenthal, based in Westchester County.

He says it's feasible thanks to free software called Asterisk. It turns a PC with a fast Internet connection into a full-fledged telephone system, with features that once cost thousands of dollars. "The barrier to entry became very low," Rosenthal says.

Asterisk was hatched in 1999 by Mark Spencer, an Auburn University computer engineering student. He also ran a tech support business for people using the free, "open source" Linux computer operating system.

"I needed a phone system. I couldn't afford to buy one, so I decided to make one," recounts Spencer, who now sells Asterisk-based services and hardware at Digium Inc. in Alabama.

Although Spencer's handiwork has spawned outfits that now sell deceptions by the minute, he insists the big phone companies could curb spoofing if they wanted. Not that he's a fan of spoofers, mind you.

"I honestly don't approve of people doing this," says Spencer, 27, who sees the world as divided between those who use technology for good and those who use it for evil. "I would rather be in that first camp, trying to do something to help people."

Kevin Coughlin covers technology. He can be reached at kcoughlin@starledger.com or (973) 392-1763.

SecurityFocus™

NEWS

< http://www.securityfocus.com/news/9061 >

VoIP hacks gut Caller I.D.

Implementation quirks in Voice over IP are making it easy for hackers to spoof Caller I.D., and to unmask blocked numbers.

By *Kevin Poulsen*, SecurityFocus Jul 6 2004 1:54PM

Caller I.D. isn't what it used to be.

Hackers have discovered that the handy feature that tells you who's calling before you answer the phone is easily manipulated through weaknesses in Voice over IP (VoIP) programs and networks. They can make their phone calls appear to be from any number they want, and even pierce the veil of Caller I.D. blocking to unmask an anonymous phoner's unlisted number.

At root, the issue is one of what happens to a nugget of authentication data when it leaves the tightly-regulated realm of traditional telephony, and passes into the unregulated domain of the Internet.

On the old-fashioned phone network, Caller I.D. works this way: your local phone company or cell phone carrier sends your "Calling Party Number" (CPN) with every call, like a return address on an envelope. Transmitted along with your CPN is a privacy flag that tells the telephone switch at the receiving end of the call whether or not to share your number with the recipient: if you have blocking on your line, the phone company you're dialing into knows your number, but won't share it with the person you're calling.

This arrangement relies on telephone equipment at both ends of the call being trusted: the phone switch providing you with dial tone promises not to lie about your number to other switches, and the switch on the receiving end promises not to reveal your number if you've asked that it be blocked. In the U.S. that trust is backed by FCC regulations that dictate precisely how telephone carriers handle CPNs, Caller I.D. and blocking. Most subscribers have come to take Caller I.D. for granted, and some financial institutions even use Caller I.D. to authenticate customers over the phone.

Despite that, the system has long been open to manipulation. "A lot of times you can offer any number you want, and carriers won't validate that," says Lance James, chief security office of Secure Science Corporation. But in the past, the power to misrepresent your number came with a high price tag: you typically had to be a business able to pay the local phone company for a high-volume digital connection. On the other side of the equation, companies who pay for toll free numbers can often access an incoming caller's phone number even if it's blocked.

Voice over IP networks, currently outside FCC regulation, place those capabilities in the hands of ordinary netizens. In a telephone interview with SecurityFocus, 21-year-old phone hacker "Lucky 225" demonstrated how he could spoof his Caller I.D. to appear to be phoning from the reporter's office. In another demonstration, the reporter phoned Lucky's associate "Natas" from a residential phone with Caller I.D. blocked. Natas was able to rattle off the unlisted phone number.

As described by Lucky, who's scheduled to give a talk on the subject at the DefCon hacker convention later this month, much Caller I.D. chicanery can be accomplished by taking advantage of implementation quirks in Voice over IP networks that try, but fail, to implement Caller I.D. properly. "There are little exploits that you can do," says Lucky. But the most powerful tool for manipulating and accessing CPN data is the open-source Linux-based PBX software Asterisk, used in combination with a permissive VoIP provider. "It's fully configurable, you can pretty much do anything you want with it," says Lucky. "That's why Voice over I.P. is changing things."

Natas used Asterisk in conjunction with the NuFone Network for his demonstration of Caller I.D. unmasking. NuFone chief Jeremy McNamara didn't return phone calls for this story.

Privacy advocates, who had reservations about Caller I.D. when it was introduced in the 90s, aren't happy that it's becoming easier to subvert. "A worse case scenario is if you have a blocked number, and you're a victim of stalking, and you're duped into calling a number the stalker set up that was routed through a VoIP line," says Jordana Beebe of the San Diego-based Privacy Right's Clearinghouse. "It could put their life in danger."

Callers with life-or-death anonymity concerns might consider spoofing just to get a little privacy. For now, Lucky says pranks among friends are the most common use that he's seen of VoIP spoofing, but he believes that identity thieves and other swindlers could have a field day. "I've used it myself to activate my own credit cards, because I never give credit card companies my real number," he says. "One simple spoof, and it's like saying, if you have the guy's phone number, that piece of information is more important than his mother's maiden name and date of birth. If you have the phone number, you don't need anything else."

<tips@securityfocus.com>

Caller ID missing in OPD

by Lindsay Huell
DM Staff Reporter
February 25, 2005

One might assume that when a police dispatcher fields a telephone call, a caller ID device would immediately track the caller's whereabouts. This, however, is not the case at the Oxford Police Department.

According to Jason Plunk, owner of Night Town in Oxford, an apparent prank call led officers to his business Monday at midnight. Plunk said the police were unable to trace the call, and they responded to a false report of a fight occurring in the parking lot.

"My impression is that someone phoned the police department representing Night Town," he said. "I am the only one who can make a judgment decision about calling the police. So I knew that the call had not been made from Night Town."

Plunk said the police told him the call came from a cell phone, but they did not know — and would have no way of discovering — who made the call.

Assistant Police Chief Mike Martin said implementing a caller ID system would be problematic.

"With as many lines as our telephone system has, we have been told that we may never be able to have caller ID," Martin said.

Martin said the police department currently has 12 lines connected with their telephone system, and the caller ID function only works with a one-line system.

In the event of a serious prank, the department has other ways of tracking calls through the Bell South telephone company.

But Martin said the majority of prank calls are made to the emergency 911 system.

Emergency 911 dispatchers do have identification capabilities.

The police department's telephone system is networked with the fire department and city hall. If the system were to be updated to incorporate caller ID, the whole network would have to be changed, Martin said.

Lori Nicholson of the Germantown Police Department in Germantown, Tenn., said their telephone system is also connected to the fire department and city hall.

They have seven emergency department lines do not contain the caller ID function either.

She said Germantown's emergency 911 lines are the only ones able to identify incoming calls.

T-Mobile security flaw in voicemail. Beware and change

T··Mobile··

By **David Ciccone**, posted Tuesday, Feb. 22nd, 2005
Reader Comments: 4
Pageviews: 20,245

Simple caller-id spoofing enables unwarranted access to your voicemail.

If any of our members of the community have Sprint or T-Mobile and you have auto voicemail login enabled, you are vulnerable to a simple hack to access your voicemail. I have auto voicemail login enabled because I hate entering my voicemail PIN number each time I want to check my messages.

The voicemail authentication system is simple. It uses caller ID to validate the originating number – if the caller ID matches your cell phone number (ie. your cell phone calling in to check your voicemail messages), it will log you in automatically.

Since the announcement of commercial caller ID spoofing systems such as CovertCall and another called TeleSpoof. For those not in-the-know, caller ID spoofing allows you to change your caller ID number to anything you like. This is extremely vulnerable and make sure you turn off auto login enabled. This is probably how they hacked into Paris Hilton's voicemail.

What is CoverCall?

Covert Call allows you to alter the caller id that is sent to the phone you are calling. It can operate just like a calling card, all for the price of a normal long distance call.

here's a scenario: Out of the office and need to contact a business associate, but don't want to reveal your private cell phone number?... Covert Call will display your business number on their caller id. No one will ever know where you are really calling from!

Manipulate the caller id, that is sent from your phone. Appear to be anyone, anywhere. This service is compatible with nearly all phones, cell phones, and even the new VoIP phones!

What is TeleSpoof?

Telespoof is offering the first domestic and international Caller I.D. spoofing service, allowing business professionals to remain anonymous when calling from anywhere in the world, to anywhere in the world. Telespoof allows you to be whoever you want to be.

Our service is for business professionals within the U.S. including, but not limited to; Private Investigators, Skip Tracers, Law Enforcement, Debt Collection Agencies, Insurance Agencies and Lawyers, allowing the freedom to choose any number to show up on the Caller I.D. display.

Telespoof operates on toll free numbers within the U.S. giving clients access from wherever they may be. No need to be in the office or at a computer to use the service. Telespoof also allows clients to place international calls with spoofed Caller I.D. permitting the technology is available within the destination country.

Quote

The only reason for the staff at Dave's iPAQ posting this is to protect the members of our community. We do not support any of these types of actions at all!

Post Your Comments

And if I purchase a throw away cell with 100minutes how are you going to track it back? That's basically how hackers do it.

Posted by **David Ciccone**, Wednesday, Feb. 23rd, 2005

The easy way to secure your voicemail from spoofed caller ID is to set it up to require you to enter your password every time.

David chose to copy and paste the ad copy directly from CovertCall and Telespoof's respective web sites. It should be noted that, even with spoofed caller ID, there is a record of the source and destination of every phone call that is placed on the US telephone network. There is no such thing as untracable phone calls.

Additionally, Telespoof was not the first company to market with caller ID spoofing.

Posted by **PI Phone**, Wednesday, Feb. 23rd, 2005

I used to have a Sanyo (5000?) cell phone years ago that allowed me to screen calls. When the phone rings, you would hit a side button that activated a local digital voice mail like introduction recording. It would appear to be a normal voice mail greating. (ot what ever you recorded) You could then interrupt to say hi after confirming it was actually someoen you want to talk to. (assuming they know to say something early, or while they are leaving a message) That's the only way I can think of to get around some of the potential headache. I havnt seen a phone with this feature though since then.

Posted by **s4czech**, Tuesday, Feb. 22nd, 2005

Everyone please note this is a very easy way to access voicemails. Paris Hilton's entire Tmobile voice mailbox is all over the internet. This could possibly be the way they got in.

Posted by **David Ciccone**, Tuesday, Feb. 22nd, 2005

But the Tupelo Police Department has four lines, all with caller ID directly linked to their department, according to a spokesperson.

Their system is not linked to any other department in the city, she said.

The technology department in charge of maintaining the telephone system for the city of Oxford was unavailable for comment.

Prank Calls Spook 'Other' Clintons

NORTH LITTLE ROCK, Ark. - Prank calls are nothing new for the famously named Bill Clinton of North Little Rock, but never as scary - or as high-tech - as this one.

Clinton, who is not related to the former president and Arkansas governor of the same name, was the victim of a dangerous p month when another person used a computer to hack into a caller-ID system and hijack Clinton's home number.

After hacking into a computer system in a process called "caller-ID spoofing," the as-yet unidentified caller made several calls home Jan. 29, telling Clinton's son he was going to disturb all the neighbors with calls that would appear to come from Clinton

The prankster then called police to make it look like it was Clinton calling, said he had a gun to someone's head and hung up armed officers to besiege Clinton's home.

Clinton had been sleeping, but his son had received the crank calls, including one saying the police were on the way. Clinton went outside to meet the police, who discovered that several calls were recorded on Clinton's own caller-ID system as having come from his own phone. That's when they realized somebody had hacked into the computer system and impersonated Clinton's telephone identification code.

Computer experts say that few people know about "spoofing" programs, which are available on the Internet and were developed so that telemarketers can bypass caller-ID systems. Coskun Bayrak of the computer science department at the University of Arkansas at Little Rock said wider knowledge of "spoofing" could encourage copycats, but could also pressure the software industry to develop improvements to cover the loopholes.

Clinton said he's received bomb threats and harassing telephone calls before, "presumably because his name is William Clinton and he lives in the Little Rock area," the police report said.

Police haven't found the culprit, but reviewed Clinton's phone records and found one suspicious call from Winterville, N.C., before the series of calls disguised as coming from Clinton's phone. The owner of t North Carolina told Winterville police that she too had been victimized by the crank caller.

The spoofer called again later the night of Jan. 29, after the police left, to see if the police had shown up. When Clinton menti an inkling the caller was from Winterville, the line went dead and the person hasn't called back, Clinton said.

Dirk Moffatt

From: Bob Lynn [boblynn@alaska.com]
Sent: Wednesday, April 06, 2005 8:48 PM
To: Rep. Bob Lynn
Subject: *****SPAM***** Caller ID Articles
Follow Up Flag: Follow up
Flag Status: Blue

You may retrieve this story by entering QuickLink# 53313

> Return to story

Scam artists dial for dollars on Internet phones
Caller ID spoofing has emerged as a useful tool for fraudsters

News Story by Andy Sullivan

MARCH 21, 2005 (REUTERS) - Internet phone services have drawn millions of users looking for rock-bottom rates. Now they're attracting identity thieves looking to turn stolen credit cards into cash.

Some Internet phone services allow scam artists to make it appear that they are calling from another phone number -- a useful trick that enables them to drain credit accounts and pose as banks or other trusted authorities, according to online fraud experts.

"It's like you've handed people an entire phone network," said Lance James, who as chief technology officer of Secure Science Corp. sees such scams on a daily basis.

The emerging scams underline the lower level of security protecting voice over IP. Traditional phone networks operate over dedicated equipment that is difficult for outsiders to penetrate. But because VoIP calls travel over the Internet, they cost much less -- but are vulnerable to the same security problems that plague e-mail and the Web. Internet worms that snarl online networks can render VoIP lines unusable, and experts at AT&T Corp. say VoIP conversations can be monitored or altered by outsiders.

Federal Trade Commission Chairman Deborah Platt Majoras

recently warned that unscrupulous telemarketers could use VoIP to blast huge numbers of voice messages to consumers, a technique known as SPIT, for "spam over Internet telephony."

All of these threats remain largely in the realm of theory, although Caller ID spoofing has emerged over the past six months as a useful tool for identity thieves and other scam artists, according to fraud experts.

Any reporter would scramble for a ringing phone that reads "White House media line" on its Caller ID display. But it's not the Bush administration on the line -- it's Ralph Echemendia, calling from a mobile phone on a remote Georgia highway. "You can see how this sort of thing could be used in a very malicious way," said Echemendia, a security instructor at the Intense School, a technology training company.

Caller ID spoofing is not prohibited by law, but the Federal Communications Commission requires telemarketers to identify themselves accurately, a spokeswoman said.

Echemendia built his own system to spoof calls, but several free or low-cost services allow even technical novices to falsify Caller ID information as well.

Debt collectors and private investigators use Camophone.com's 5-cents-per-call service to trick people into answering the phone, according to messages posted on a discussion board. Traveling salesmen say the service comes in handy when they want clients to return calls to the main office, rather than to their motel room.

James said criminal uses of Caller-ID spoofing have become more common.

Wire-transfer services like Western Union require customers to call from their home phone when they want to transfer money in an effort to deter fraud -- a barrier easily sidestepped by any identity thief using a Caller-ID spoofing service. Fraud rings can now transfer money directly out of stolen credit card accounts, rather than buying merchandise and reselling it, he said.

Western Union spokeswoman Danielle Periera said the company has no other way to verify that transfer requests are valid. "We try hard to stay one step ahead of them and recognize that scam artists are sophisticated and often change their schemes," she said.

Criminals can use Caller ID spoofing to listen to other people's voice mail, James said, especially when those accounts are not protected by passwords.

They also have begun to use the technology to make it appear that they are calling from a bank or other financial institution, said Dave Jevans, who chairs the Anti-Phishing Working Group, a banking industry task force. That helps them convince consumers to divulge account numbers, passwords and other sensitive information in a scam that echoes the "phishing" e-mails that have become common, he said.

VoIP industry pioneer Jeff Pulver, whose Free World Dialup service can be used to spoof calls, said he couldn't prevent abuse of his system. But the problem will likely recede as companies like VeriSign Inc. and NeuStar Inc. develop ways to verify online identities, he said. "We're not there yet, but we're going to get there," Pulver said.

Internet phones a hacking risk?

Low-cost services may attract identity thieves looking to turn stolen credit cards into cash.
March 18, 2005 3:45 PM EST

WASHINGTON (Reuters) - Internet phone services have drawn millions of users looking for rock-bottom rates. Now they're also attracting identity thieves looking to turn stolen credit cards into cash.

Some Internet phone services allow scam artists to make it appear that they are calling from another phone number -- a useful trick that enables them to drain credit accounts and pose as banks or other trusted authorities, online fraud experts say.

"It's like you've handed people an entire phone network," said Lance James, who as chief technology officer of Secure Science Corp. sees such scams on a daily basis.

The emerging scams underline the lower level of security protecting Voice Over Internet Protocol, or VOIP, the Internet-calling standard that has upended the telecommunications industry over the past several years.

Traditional phone networks operate over dedicated equipment that is difficult for outsiders to penetrate. Because VOIP calls travel over the Internet, they cost much less but are vulnerable to the same security problems that plague e-mail and the Web.

Internet worms that snarl online networks can render VOIP lines unusable, and experts at AT&T (Research) say VOIP conversations can be monitored or altered by outsiders.

Federal Trade Commission Chairman Deborah Platt Majoras recently warned that unscrupulous telemarketers could use VOIP to blast huge numbers of voice messages to consumers, a technique

known as SPIT, for "spam over Internet telephony."

All of these threats remain largely in the realm of theory. Caller ID spoofing, on the other hand, has emerged over the past six months as a useful tool for identity thieves and other scam artists, according to fraud experts.

President Bush on the line

Any reporter would scramble for a ringing phone that reads "White House media line" on its caller ID display.

But it's not the Bush administration on the line -- it's security instructor Ralph Echemendia, calling from a mobile phone on a remote Georgia highway.

"You can see how this sort of thing could be used in a very malicious way," said Echemendia, a security instructor at the Intense School, a technology training company.

Caller ID spoofing is not prohibited by law, but the Federal Communications Commission requires telemarketers to identify themselves accurately, a spokeswoman said.

Echemendia built his own system to spoof calls, but several free or low-cost services allow even technical novices to falsify caller ID information as well.

Debt collectors and private investigators use Camophone.com's 5-cents-per-call service to trick people into answering the phone, according to messages posted on a discussion board.

Traveling salesmen say the service comes in handy when they want clients to return calls to the main office, rather than their motel room.

James said criminal uses of caller-ID spoofing have become common over the last six months.

Wire-transfer services like Western Union (Research) require customers to call from their home phone when they want to transfer money in an effort to deter fraud -- a barrier easily sidestepped by any identity thief using a caller-ID spoofing service.

Fraud rings can now transfer money directly out of stolen credit-card accounts, rather than buying merchandise and reselling it, he said.

Western Union spokeswoman Danielle Periera said the company has no other way to verify that transfer requests are valid.

"We try hard to stay one step ahead of them and recognize that scam artists are sophisticated and often change their schemes," she said.

Criminals can use caller-ID spoofing to listen to other people's voice mail, James said, especially when those accounts are not protected by passwords.

They also have begun to use the technology to make it appear that they are calling from a bank or other financial institution, said Dave Jevans, who chairs the Anti-Phishing Working Group, a banking-

industry task force.

That helps them convince consumers to divulge account numbers, passwords and other sensitive information in a scam that echoes the "phishing" e-mails that have become common, he said.

VOIP industry pioneer Jeff Pulver, whose Free World Dialup service can be used to spoof calls, said he couldn't prevent abuse of his system.

The problem will likely recede as companies like VeriSign Inc. (Research) and NeuStar Inc. develop ways to verify online identities, he said: "We're not there yet, but we're going to get there." ■

what's this?

Caller-ID Spoofing: 'Appallingly Bad Idea'

By Erika Morphy
NewsFactor Network
September 2, 2004 1:26PM

A new software system that allows users to fool telephone caller-ID into displaying false numbers opens the door to a variety of abuses. "What an appallingly bad idea," says Graham Cluley of security firm Sophos.

COMPLETE STORY

A startup company has developed a software system that allows users to spoof a caller-ID number in order to trick the telephone-call recipient into answering the phone.

Developed by Star38, the service will be marketed solely to collection agencies, private investigators and the police, according to statements made by the company.

The system itself is said to be easy to use, with the user typing in the recipient's number and the number he or she would like to appear on the caller ID.

Appallingly Bad

Critics of the system -- and there are many, even outside the usual privacy/consumer-advocacy brigade -- find the technology frightening. "What an appallingly bad idea," says Graham Cluley, managing consultant for security and antivirus firm Sophos. "It reminds me of the hacker-driven spam and phishing scams that have taken over the Internet," he told NewsFactor.

In fact, it is a much worse form of deception than Internet fraud, says John Morris, staff counsel for the Center for Democracy & Technology, a Washington-based public-policy organization with a focus on technology.

Reasonable Expectation

"On the Internet, most people understand that the identity of someone who is sending an e-mail may easily be spoofed," Morris told NewsFactor. "But the phone, historically, has had a different set of expectations or assumptions. Most people that have Caller ID assume the number listed is accurate."

In news accounts, Star38 has emphasized its intent to limit the technology to the police, collection agencies and private investigators.

However, "there really isn't anything that will prevent this kind of technology from being used by other firms, such as telemarketers, now that it has been developed," Morris says, adding, "in this age of identity theft, we are skeptical that spoofing other phone numbers on Caller ID is a desirable development."

One scenario, Morris suggests, might be someone purporting to call from a distant relative's house, claiming the person had an accident.

Potential for Abuse

But even assuming that Star38 keeps the technology in the hands of collection agencies, private investigators and the police, there still would be cause for worry.

While the police may well have a legitimate need for the technology in criminal investigations, the potential for abuse by collection agencies and PIs is huge.

For example, there have been cases of stalkers retaining private investigators to find victims who went into hiding.

As for collection agencies, the potential for abuse is even wider. "We don't understand what purpose a legitimate collections agency would have in hiding its identity," Morris says.

The typical example, of course, is an agency that uses the system to get a phone-shy debtor to answer the call and coax him or her into paying the debt.

Collection agencies, though, have not entirely shed their less-than-upstanding practices since the passage of the Fair Debt Collection Practices Act. Recently, one firm was fined for continually contacting and harassing a debtor's neighbors -- a practice clearly illegal under FDCP.

Over the Line

More often, though, when these agencies go over the line, it is a little more discreet.

Recently, a legal journal reported that a court found a collection agency had made false statements as to the time limit of a debt-discount offer; reportedly, the firm told the debtor she had 30 days to make a payment if she wanted to get a percentage taken off her debt. In truth there was no time limit of 30 days -- a deception prohibited by the law.

Which brings us back to Star38's latest contribution to the Internet age. In his first take on the system, Morris says he does not believe the system itself violates the tenets of FDCP. When it gets in the hands of the agencies, though, that may be a different story.

"I do believe we will see some deceptive practices on the part of the agencies that will violate the spirit of FDCP," he says.

Caller ID: Do you really know who's calling?

By Ben Charny CNET News.com August 30, 2004, 4:37 PM PT

Your Caller ID feature may no longer be telling the truth.

This week, a company is launching technology that will make it possible for someone to choose what appears on phones that have Caller ID, the feature for displaying identifying information about an incoming call.

It could be a different phone number, or even a few words, said Jason Jepson, founder of Star38, which has developed the commercial Caller ID spoofing service. Sales of Star38 will be limited to licensed private investigators and collection agencies, Jepson said. The service will cost $20 a month plus airtime charges.

The technique for replacing the usual bits of identifying information, such as ph

Caller ID Spoofing Service Debuts Sept. 1, 2004

Star38's service disguises who is making the call but will only be sold to collection agencies, private investigators, and law-enforcement personnel.
By Paul Travis
InformationWeek

A service introduced Wednesday can send misleading information to phones that display Caller ID information, which is used to identify who is placing a call before the called party answers the phone.

The service will only be sold to collection agencies, private investigators, and law-enforcement personnel, says Jason Jepson, founder and CEO of Star38. "This is not for public use," he says. "We just opened today and we've gotten 600 inquiries so far."

The service will let collection agencies and others avoid breaking laws that prohibit them from using phony phone numbers when they try to collect money, Jepson says. His service will provide them with a legitimate phone number--but one that can't be associated with the actual caller, he says.

Potential customers must go to the Star38 Web site and download an application. They must provide copies of business licenses and other proof that they are the types of businesses that Jepson wants to serve. Once that information is verified--a process that can take seven to 10 days--a customer is granted access to the Star38 service.

For a collection agency to use the service, it would log on to the Star38 server and telephone-switching system and fill out a form with the target's phone number. The Star38 system places the call and, if answered, automatically routes the call to the collection agency's call center or other specified phone number. If the target isn't home and calls back later, the call will be automatically routed to the collection agency's phone.

Jepson says he has purchased several phone numbers from local telephone companies; one of these is what pops up on the Caller ID screens used by many consumers to see who's calling them.

"We are providing collection agencies with another option," Jepson says. "Our service will completely document each call, including how long it took, when it was made, and data like that." The service costs $20 per month, plus 7 to 10 cents per minute for phone charges.

one number and name, that accompany inbound calls was discovered a few years ago by hackers. Privacy advocates fear that in the wrong hands, commercial services have the potential to be abused. For instance, telemarketers could use technologies similar to Star38's to trick people into answering a call that looks like a familiar phone number.

Star38 aims to overcome the stigma created by earlier pranksters and thieves. "Unfortunately, what's happened is some hackers have got to it first and gave it a bad name," Jepson said. "If they step back and see the forest through the trees, they'd realize what they are doing is hard and illegal. What we are doing is neither."

The company plans to explore other markets as well. For example, Jepson said he's begun talks with Musicphone, a San Francisco-based service that lets people send songs, along with personalized messages, to any kind of phone--cellular or standard.

Musicphone wants to use Star38's software to send even more information about certain artists, he said. A Musicphone representative could not immediately be rea

==========----------

Juneau Office
130 Seward St #209
Juneau, Alaska 99801
Phone: (907) 586-3650
Fax: (907) 463-4493
www.andvsa.org

ANDVSA
Alaska Network on Domestic Violence & Sexual Assault

Sitka Office
PO Box 6631
Sitka, Alaska 99835
Phone: (907) 747-7545
Fax: (907)747-7547

April 10, 2006

The Honorable Bob Lynn
State House of Representatives
Alaska State Capitol
Juneau, AK 99801-1182

Dear Representative Lynn:

The Alaska Network on Domestic Violence & Sexual Assault is a statewide coalition of member shelter and community based programs that provide direct services and advocacy for victims of domestic violence and sexual assault. We would like to thank you for introducing House Bill 308, "An Act relating to false caller identification", and offer our support.

Victims of interpersonal violence are often harassed and stalked through the phone system by perpetrators. One very important protection that victims use is caller ID to prevent unknown numbers from reaching them. This is a key safety feature for victims because when perpetrators reach them to threaten, cajole, "guilt trip", or even beg forgiveness, the emotional effects can be devastating.

One easy query on the internet finds the ad: "*Free Voice Changer & Call Recording: Call anyone and Fake your Caller ID.*" It is chilling to know that perpetrators have such easy access to these threatening tools and that they currently face no consequence for using it.

The Network strongly supports this legislation to make use of this software illegal and we thank you for your leadership in addressing this issue.

Please let me know if I can offer other support for this legislation.

Sincerely,

Peggy Brown
Executive Director

CONGRESSMAN
Tim Murphy

Working For The 18th District Of Pennsylvania

- Biography
- About The District
- NewsRoom
- Issues
- Multimedia
- Constituent Services
- Photo Gallery
- Contact Tim
- District Links
- Visit Washington DC
- Email Updates

Your Email Address

Subscribe

Kid's Page

Biography

Home / Biography / **Biography**

At a young age, Tim Murphy learned that hard work is the key to success. He was one of eleven children, born to working class parents who stressed the importance of family, education and self-reliance.

He worked his way through college and graduate school, eventually earning a PhD in psychology. He started a family of his own, opened a small business, went to work at hospitals across Western Pennsylvania, consulted for schools and Head Start, and taught at the University of Pittsburgh. He authored several publications, including two books: the award-winning "The Angry Child," and "Overcoming Passive-Aggression." During this time, he became widely known as "Dr. Tim" through regular appearances on local and national radio and television.

From 1997-2002 he served in the Pennsylvania State Senate. As an elected official, and one of very few with a health care background, he found that he could help more families. He penned the state's historic Patient Bill of Rights and increased funding for medical research, while consistently supporting responsible fiscal management of government to promote job creation and reduce the tax burden on families.

He took this commitment to Congress when he began representing the people of the 18th district of Pennsylvania in 2003.

He got to work immediately in Washington. In just his second term, Congressman Murphy was named a member of the Energy and Commerce Committee. He has three subcommittee assignments: Commerce, Trade, and Consumer Protection; Energy and Air Quality, and Environment and Hazardous Materials. Tim quickly emerged as a leader among his peers and was elected by his colleagues to serve as President of the 2003 class. He also is recognized as a leader in Congress on mental health issues, and serves as Co-chair of both the Congressional Mental Health Caucus, and the 21st Century Healthcare Caucus.

During his tenure in the state Senate, he served as chair of the Pennsylvania Committee on Aging and Youth. He utilized this unique experience to ensure the recent Medicare Prescription Drug Act would work in conjunction with Pennsylvania's PACE program. As a result, it is estimated that PACE will save up to $150 million over the next two years.

Tim Murphy makes it a priority to bring together business and community leaders to focus on new and innovative ways to retrain our job force to better position Western Pennsylvania to face the challenges of the new world economy. Representing a district with a large number of veterans – and a member of the Sons of American Legion himself, he firmly supports our armed services and shows commitment to our veterans by working to expand benefits and improve services to veterans' health care.

Nan and Tim Murphy reside in Upper St. Clair with their daughter, Bevin who is currently attending college. They attend St. Thomas More Catholic Church in Bethel Park.

He earned a bachelors degree from Wheeling Jesuit University, a master's degree from Cleveland State University, and a his PhD from the University of Pittsburgh.

A fierce proponent of community involvement, he is a strong advocate of the Rails to Trails programs, an active participant in events for Habitat to Humanity and member of several Rotary Clubs and Chambers of Commerce.

CONGRESSMAN
Tim Murphy
Working For The 18th District Of Pennsylvania

- Biography
- About The District
- NewsRoom
- Issues
- Multimedia
- Constituent Services
- Photo Gallery
- Contact Tim
- District Links
- Visit Washington DC
- Email Updates

Your Email Address
Subscribe

Kid's Page

Photo Gallery

Home / Photos / **Photo**

Veterans' Affairs

Rep. Murphy attends a hearing at the House Committee on Veteran's Affairs.

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

CONGRESSMAN
Tim Murphy
Working For The 18th District Of Pennsylvania

- Biography
- About The District
- NewsRoom
- Issues
- Multimedia
- Constituent Services
- Photo Gallery
- Contact Tim
- District Links
- Visit Washington DC
- Email Updates

Your Email Address
Subscribe

Kid's Page

Contact Tim

Home / Contact / **Contact**

Email Congressman Murphy

D.C. Office

Phone (202) 225-2301
Fax: (202) 225-1844
322 Cannon House Office Building
Washington, DC 20515

Chief of Staff: Susan Mosychuk

Legislative Director: Michael Layman

Communications Director: Mark Carpenter

Scheduler: Morgan Jones

Senior Legislative Assistant: Michael Baxter

Legislative Assistant (Energy): Gregory Lovejoy

Legislative Correspondent: Brandon Fisher

Staff Assistant: Kishore Thota

Main District Office

Phone: (412) 344-5583
Fax: (412) 429-5092
504 Washington Rd
Pittsburgh, PA 15228

District Director: Nick Redondo

Field Director: Nick Sherman

District Scheduler: Jayne O'Shaughnessy

Special Projects Coordinator: Emily Campbell

Congressional Aide: Aaron Houser

Congressional Aide: Martha McGrath

Westmoreland District Office

Phone: (724) 850-7312
Fax: (724) 850-7315
2040 Frederickson Place
Greensburg, PA 15601

Westmoreland County Director: Lou Lazzaro

Capitol Mail is Delayed

Due to the various screening procedures set in place since the anthrax incidents our Washington office is receivir mail 2-3 weeks late.

Home | Biography | About The District | NewsRoom | Issues | Constituent Services | Photo Gallery
Contact Tim | District Links | Visit Wasnington DC | Kid's Page | Privacy Policy

SpoofCard™

SpoofCard calling cards offers you the ability to change what someone see on their caller ID display when they receive a phone call.

Key Benefits: Make calls truly private, Ability to record calls, Change your voice, Fun and inexpensive, Easy to use and fast to set up! **Instant Access!**

Control Panel Login

Calling Card Pin:

ENTER Lost/Forgot PIN

- BUY INSTANT CALLING MINUTES
- ADD MONEY TO EXISITNG CARD
- FREQUENTLY ASKED QUESTIONS
- INTERNATIONAL RATES
- CUSTOMER SERVICE
- PRIVACY POLICY

Purchase $10 Calling Card

- 60 Minutes USA Talk Time
- Caller ID Spoofing
- Free Call Recording
- Customer Service Support

BUY NOW

Purchase $20 Calling Card

- 120 Minutes USA Talk Time
- Caller ID Spoofing
- Free Call Recording
- Customer Service Support

BUY NOW

Purchase $40 Calling Card

- 240 Minutes USA Talk Time
- Caller ID Spoofing
- Free Call Recording
- Customer Service Support

MORE INFO

SPOOFCARD FEATURES:

- **Caller ID Spoofing**
- **Voice Changer**
- **Call Recording**
- **Web Control Panel**

No computer needed! Simply dial the toll free number from the calling card you purchase.

1.Enter your pin number.
3. Enter Destination number.
2. Enter Any Caller ID Number you wish to display.
4. Choose the voice you would like to use.
5. Your call is connected using the specified Caller ID Number.

As an added bonus, we offer you the option to record your conversation for **FREE** which you can later retrive by logging-in to your control panel or calling our 800 number from anywhere.

In addition, we also offer the ability to change your voice to sound like a man, a women or yourself for **FREE**.

SpoofCard™

Frequently Asked Questions

How does SpoofCard work?

SpoofCard is a regular calling card. SpoofCard can be accessed through our dedicated toll free number where a user enters their pin number, desired Caller ID and the number they would like to call. The call is then placed instantly without the need to ever be online or at a computer.

Does SpoofCard offer call recording?

Yes, SpoofCard offers FREE call recording with instant access via your online control panel or by calling the toll free number.

How can I change my voice?

SpoofCard offers the ability to select a Male or Female voice when making a call. The feature works in real-time and allows the caller to speak in a normal tone while the person on the other end will hear the changed voice.

Are there any restrictions with using SpoofCard?

To ensure SpoofCard is used within our User Agreement, we have implemented several security measures which includes the inability to dial toll free numbers or 911. Federal Regulations prohibit the use of our technology by telemarketers or debt collectors to hide or falsify the telephone number from which they are calling. You must agree that you will not use the SpoofCard in violation of this or any other applicable law or regulation.

What are the advantages of Caller ID spoofing?

Caller ID spoofing gives business professionals the ability to manipulate their identity to their choosing and stay anonymous. Caller ID spoofing is also valuable in defeating popular telephone services such as "*57 Call Trace", "*69 Last Call Return", "Anonymous Call Rejection" and "Detailed Billing". Private Investigators will find Caller ID spoofing valuable for pretext calls.

Who may sign up for your service?

Our target market consists of, but is not limited to, businesses such as: Private Investigators, Law Enforcement, Skip Tracers, Insurance Agencies and Lawyers.

Does SpoofCard store my credit card information?

No, SpoofCard never receives your credit card information from our payment processors, keeping your information secure.

Can I call internationally?

Currently we only support the option to call within the United States and Canada

Control Panel Login

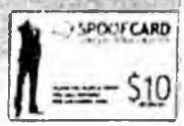
Calling Card Pin:

ENTER Lost/Forgot PIN

- BUY INSTANT CALLING MINUTES
- ADD MONEY TO EXISITNG CARD
- FREQUENTLY ASKED QUESTIONS
- INTERNATIONAL RATES
- CUSTOMER SERVICE
- PRIVACY POLICY

Purchase $10 Calling Card

- 60 Minutes USA Talk Time
- Caller ID Spoofing
- Free Call Recording
- Customer Service Support



BUY NOW

Purchase $20 Calling Card

- 120 Minutes USA Talk Time
- Caller ID Spoofing
- Free Call Recording
- Customer Service Support

BUY NOW

Purchase $40 Calling Card

- 240 Minutes USA Talk Time
- Caller ID Spoofing
- Free Call Recording
- Customer Service Support

MORE INFO

Can we send any number as the Caller ID and does it have to be 10 digits long?

You may send any number as the Caller ID. Within the U.S. the number should be 10 digits long (NXX-XXX-XXXX) to guarantee properly delivery, but you may pass numbers of variable length such as "0", "411" or "12345". Results may vary based on location and the receiving ends telephone provider.

How do we sign up?

To sign up please visit the Buy Now Page.

LEGISLATIVE RESEARCH REPORT

MARCH 10, 2005

REPORT NUMBER 05.220

LEGISLATION IN OTHER STATES: CALLER ID FALSIFICATION, OR "SPOOFING"

PREPARED FOR REPRESENTATIVE BOB LYNN

BY CHUCK BURNHAM, LEGISLATIVE ANALYST

You asked about caller ID falsification, or "spoofing." Specifically, you asked if any states have considered legislation that would make illegal "spoofing"—that is, using electronic means to cause caller ID systems to display false information. Further, you asked how a law making this practice illegal in Alaska might be crafted.

In mid-2004, a flurry of media interest surrounding caller ID systems was generated when hackers discovered that the systems could be manipulated, through fairly simple means, to display incorrect information on a receiving party's caller ID display. Concern over the systems' vulnerability intensified later in the year when a company announced plans to offer a commercial product that would enable purchasers to spoof caller ID systems at will. Although the vendor eventually opted to offer the product only to law enforcement agencies, which can use the tool as an incognito means to contact and locate wanted individuals, privacy advocates and consumer groups voiced concern that the misuse of such technology could be instrumental in identity theft schemes and other inappropriate or illegal actions.

Our research identified only one state, New York, that has thus far considered legislation specifically related to caller ID spoofing.[1] We include, as Attachment A, copies of two bills currently under consideration in New York.

Although legislation has not yet been widely considered specifically with regard to spoofing Caller ID systems, under certain circumstances such chicanery may be illegal in a number of states under laws intended to address other issues. In 2002-2003, for example, a number of states enacted legislation creating "do not call lists." Generally, these laws require telemarketers to remove from their databases the telephone numbers of people appearing on the list, thereby

[1] Our research included Lexis database searches of the current laws of the fifty states and of all state legislation introduced in the years 2003-2005 using the terms "caller ID" and "caller identification." There may be states with laws of similar practical application, but worded such that our Lexis queries did not identify them.

allowing consumers to "opt out" of receiving soliciting phone calls. Some such laws included other restrictions on the business practices of telemarketers with regard to caller ID systems. Michigan, for instance, passed Act 612 (2002), which included the following section:

> A telephone solicitor shall not intentionally block or otherwise interfere with the caller ID function on the telephone of a residential telephone subscriber to whom a telephone solicitation is made so that the telephone number of the caller is not displayed on the telephone of the residential telephone subscriber.

The Michigan law defines "telephone solicitation" as using "any voice communication over a telephone for the purpose of encouraging the recipient of the call to purchase, rent, or invest in goods or services during that telephone call . . ." It is unclear, therefore, to what degree spoofing caller ID systems for purposes other than solicitation may be covered by this law. We include, as Attachment B, a copy of Michigan Public Act 612 (2002).

We are unable to identify a model law as a basis for drafting such legislation in Alaska perhaps because no direct precedent yet exists for making illegal the falsification of caller ID systems. You may want to contact Legal Services for more information on this matter.

I hope you find this information to be useful. Please do not hesitate to contact us if you have questions or need additional information.

Attachment A

New York Assembly Bill 1603 (2005)

New York Senate Bill 1075 (2005)

2005 NY A.B. 1603

NEW YORK 228TH ANNUAL LEGISLATIVE SESSION

ASSEMBLY BILL 1603
2005-2006 REGULAR SESSIONS
JANUARY 21, 2005
INTRODUCED BY M. OF A. SWEENEY, WEISENBERG, CLARK, A. COHEN, SEDDIO, BRADLEY, HOOPER, AUBERTINE, PHEFFER -- MULTI-SPONSORED BY -- M. OF A. AUBRY, M. COHEN, COLTON, L. DIAZ, GALEF, GORDON, GRANNIS, HIKIND, JOHN, KOON, LAFAYETTE, MAGEE, MAYERSOHN, PEOPLES, PERRY, P. RIVERA, ROBINSON, SCHIMMINGER, STRINGER, TOWNS -- READ ONCE AND REFERRED TO THE COMMITTEE ON CORPORATIONS, AUTHORITIES AND COMMISSIONS

2005 Bill Text NY A.B. 1603

VERSION-DATE: January 21, 2005

SYNOPSIS: AN ACT to amend the public service law, in relation to defining and prohibiting caller ID scamming

NOTICE: [A> UPPERCASE TEXT WITHIN THESE SYMBOLS IS ADDED <A]

TEXT: THE PEOPLE OF THE STATE OF NEW YORK, REPRESENTED IN SENATE AND ASSEMBLY, DO ENACT AS FOLLOWS:

Section 1. The public service law is amended by adding a new section 92-g to read as follows:

[A> SECTION 92-G. CALLER ID SCAMMING. 1. DEFINITIONS. AS USED IN THIS SECTION, THE FOLLOWING TERMS SHALL HAVE THE FOLLOWING MEANINGS: <A]

[A> (A) "CALLER ID EQUIPMENT" SHALL MEAN ANY DEVICE THAT IS PART OF OR ATTACHED TO A TELEPHONE RECEIVER THE PURPOSE OF WHICH IS TO DISPLAY OR OTHERWISE INDICATE THE TELEPHONE NUMBER OR OTHER IDENTIFIER OF THE PERSON OR TELEPHONE INITIATING THE CALL; <A]

[A> (B) "CALLER ID SCAM" SHALL MEAN ANY SCHEME, PLAN, SUBTERFUGE OR DEVICE INTENDED TO CAUSE THE CALLER ID EQUIPMENT USED BY ANY PERSON RECEIVING A TELEPHONE COMMUNICATION TO INDICATE THAT SUCH TELEPHONE COMMUNICATION WAS INITIATED AT A TELEPHONE NUMBER OTHER THAN THE NUMBER OF THE TELEPHONE BEING USED BY THE CALLER; AND <A]

[A> (C) "TELEPHONE COMMUNICATION" SHALL MEAN "TELECOMMUNICATION SERVICES" AS DEFINED IN PARAGRAPH (G) OF SUBDIVISION ONE OF SECTION ONE HUNDRED EIGHTY-SIX-E OF THE TAX LAW. <A]

[A> 2. IT SHALL BE UNLAWFUL FOR A PERSON INITIATING A TELEPHONE COMMUNICATION TO ENGAGE IN OR USE ANY CALLER ID SCAM WITH THE INTENT TO DEFRAUD A PERSON RECEIVING SUCH TELEPHONE COMMUNICATION. <A]

[A> 3. IT SHALL BE UNLAWFUL FOR A TELEPHONE SOLICITOR IN MAKING OR CAUSING TO BE MADE A CONSUMER TELEPHONE CALL TO USE ANY CALLER ID SCAM WITH THE INTENT TO DEFRAUD A CONSUMER RECEIVING SUCH CONSUMER TELEPHONE CALL. FOR THE PURPOSES OF THIS SUBDIVISION THE TERMS "TELEPHONE SOLICITOR" AND "CONSUMER TELEPHONE CALL" SHALL HAVE THE MEANINGS ASSIGNED TO SUCH TERMS IN SUBDIVISION ONE OF SECTION THREE HUNDRED NINETY-NINE-P OF THE GENERAL BUSINESS LAW. <A]

[A> 4. THE COMMISSION UNDER THE DIRECTION OF THE CHAIRMAN IS HEREBY EMPOWERED TO ESTABLISH AND ADOPT RULES AND REGULATIONS TO EFFECTUATE THE PROVISIONS OF THIS SECTION. <A]

[A> 5. ANY VIOLATION OF THIS SECTION IS PUNISHABLE BY A CIVIL PENALTY OF NOT MORE THAN ONE THOUSAND FIVE HUNDRED DOLLARS. <A]

Section 2. This act shall take effect on the one hundred eightieth day after it shall have become a law; provided, however that effective immediately, the addition, amendment and/or repeal of any rule or regulation necessary for the implementation of this act on its effective date are authorized and directed to be made and completed on or before such effective date.

SPONSOR: Sweeney

SUBJECT: TELEMARKETING (90%); RESIDENTIAL TELEPHONE SERVICE (90%); FRAUD & FINANCIAL CRIME (90%); LEGISLATION (78%); LEGISLATORS (78%); TAX LAW (73%); TAXES & TAXATION (73%); FINES & PENALTIES (73%); TELECOMMUNICATIONS (55%);

LOAD-DATE: January 26, 2005

2005 NY S.B. 1075

JANUARY 24, 2005
INTRODUCED BY SENS. ALESI, LITTLE, MALTESE, TRUNZO -- READ TWICE AND ORDERED PRINTED, AND WHEN PRINTED TO BE COMMITTED TO THE COMMITTEE ON CONSUMER PROTECTION

2005 Bill Text NY S.B. 1075

VERSION: Introduced

VERSION-DATE: January 24, 2005

SYNOPSIS: AN ACT to amend the general business law, in relation to preventing certain persons from fraudulently impersonating others on caller ID

NOTICE: [A> UPPERCASE TEXT WITHIN THESE SYMBOLS IS ADDED <A]

TEXT: THE PEOPLE OF THE STATE OF NEW YORK, REPRESENTED IN SENATE AND ASSEMBLY, DO ENACT AS FOLLOWS:

Section 1. The general business law is amended by adding a new section 399-cc to read as follows:

[A> SECTION 399-CC. FRAUDULENT IMPERSONATION BY CALLER ID. 1. AS USED IN THIS SECTION, THE FOLLOWING TERMS SHALL HAVE THE FOLLOWING MEANINGS: <A]

[A> A. "BOARD" SHALL MEAN THE CONSUMER PROTECTION BOARD; AND <A]

[A> B. "PERSON" MEANS ANY NATURAL PERSON, ASSOCIATION, PARTNERSHIP, FIRM, CORPORATION, LIMITED LIABILITY COMPANY AND ITS AFFILIATES OR SUBSIDIARIES OR OTHER BUSINESS ENTITY. <A]

[A> 2. IT SHALL BE UNLAWFUL FOR ANY PERSON TO FRAUDULENTLY USE STAR #38 OR ANY OTHER SUCH METHOD OR FUNCTION TO CHOOSE THE NAME AND NUMBER, OTHER THAN SUCH PERSON'S ORIGINAL NAME AND NUMBER, WHICH WOULD APPEAR ON THE CALLER ID BOX OF THE PERSON CALLED. <A]

[A> 3. ANY COMPANY THAT PROVIDES LOCAL TELEPHONE DIRECTORIES TO CUSTOMERS IN THIS STATE SHALL INFORM ITS CUSTOMERS OF THE PROVISIONS OF THIS SECTION BY MEANS OF PUBLISHING A NOTICE IN SUCH LOCAL TELEPHONE DIRECTORIES. <A]

[A> 4. THE BOARD SHALL PRESCRIBE RULES AND REGULATIONS TO ADMINISTER THIS SECTION. <A]

Section 2. This act shall take effect on the one hundred eightieth day after it shall have become a law.

SPONSOR: Alesi

SUBJECT: IMPERSONATION (93%); CONSUMER PROTECTION (90%); LEGISLATORS (90%); LEGISLATION (78%);

LOAD-DATE: January 27, 2005

Attachment B

Michigan Public Act 612 of 2003 (introduced as House Bill 4042)

MICHIGAN 91ST LEGISLATURE -- 2002 REGULAR SESSION

HOUSE BILL 4042
(Act 612, Public Acts of 2002)

2002 Mi. ALS 612; 2002 Mi. P.A. 612; 2001 Mi. HB 4042

The People of the State of Michigan enact:

TITLE

An act to prescribe the rights and duties of parties to home solicitation sales; to regulate certain telephone solicitation; to provide for the powers and duties of certain state officers and entities; and to prescribe penalties and remedies.

Sec. 1. As used in this act:

(a) "Home solicitation sale" means a sale of goods or services of more than $ 25.00 in which the seller or a person acting for the seller engages in a personal, telephonic, or written solicitation of the sale, the solicitation is received by the buyer at a residence of the buyer, and the buyer's agreement or offer to purchase is there given to the seller or a person acting for the seller. Home solicitation sale does not include any of the following:

(i) A sale made pursuant to a preexisting revolving charge account.

(ii) A sale made pursuant to prior negotiations between the parties at a business establishment at a fixed location where goods or services are offered or exhibited for sale.

(iii) A sale or solicitation of insurance by an insurance agent licensed by the commissioner of insurance.

(iv) A sale made at a fixed location of a business establishment where goods or services are offered or exhibited for sale.

(v) A sale made pursuant to a printed advertisement in a publication of general circulation.

(vi) A sale of services by a real estate broker or salesperson licensed by the department of consumer and industry services.

(vii) A sale of agricultural or horticultural equipment and machinery that is demonstrated to the consumer by the vendor at the request of either or both of the parties.

(b) "Fixed location" means a place of business where the seller or an agent, servant, employee, or solicitor of that seller primarily engages in the sale of goods or services of the same kind as would be sold at the residence of a buyer.

(c) "Business day" means Monday through Friday and does not include Saturday, Sunday, or the following business holidays: New Year's day, Martin Luther King's birthday, Washington's birthday, Memorial day, Independence day, Labor day, Columbus day, Veterans' day, Thanksgiving day, and Christmas day.

(d) "Federally insured depository institution" means a state or national bank, state or federal savings bank, state or federal savings and loan association, or state or federal credit union that holds deposits insured by an agency of the United States.

(e) As used in only the definition of home solicitation sales, "goods or services" does not include any of the following:

(i) A loan, deposit account, or trust account lawfully offered or provided by a federally insured depository institution or a subsidiary or affiliate of a federally insured depository institution.

(ii) An extension of credit that is subject to any of the following acts:

(A) The mortgage brokers, lenders, and servicers licensing act, *1987 PA 173*, MCL 445.1651 to 445.1684.

(B) The secondary mortgage loan act, *1981 PA 125*, MCL 493.51 to 493.81.

(C) The regulatory loan act, *1939 PA 21*, MCL 493.1 to 493.24.

(D) The consumer financial services act, *1988 PA 161*, MCL 487.2051 to 487.2072.

(E) *1984 PA 379*, MCL 493.101 to 493.114.

(F) The motor vehicle sales finance act, 1950 (Ex Sess) PA 27, MCL 492.101 to 492.141.

(iii) A sale of a security or interest in a security that is subject to the uniform securities act, *1964 PA 265*, MCL 451.501 to 451.818.

(f) "Written solicitation" means a postcard or other written notice delivered to a buyer's residence that requests that the buyer contact the seller or seller's agent by telephone to inquire about a good or service, unless the postcard or other written notice concerns a previous purchase or order or specifies the price of the good or service and accurately describes the good or service.

(g) "ADAD" or "automatic dialing and announcing device" means any device or system of devices that is used, whether alone or in conjunction with other equipment, for the purpose of automatically selecting or dialing telephone numbers.

(h) "Commission" means the public service commission.

(i) "Do-not-call list" means a do-not-call list of consumers and their residential telephone numbers maintained by the commission, by a vendor designated by the commission, or by an agency of the federal government, under section 1a.

(j) "Existing customer" means an individual who has purchased goods or services from a person, who is the recipient of a voice communication from that person, and who either paid for the goods or services within the 12 months preceding the voice communication or has not paid for the goods and services at the time of the voice communication because of a prior agreement between the person and the individual.

(k) "Person" means an individual, partnership, corporation, limited liability company, association, governmental entity, or other legal entity.

(l) "Residential telephone subscriber" or "subscriber" means a person residing in this state who has residential telephone service.

(m) "Telephone solicitation" means any voice communication over a telephone for the purpose of encouraging the recipient of the call to purchase, rent, or invest in goods or services during that telephone call. Telephone solicitation does not include any of the following:

(i) A voice communication to a residential telephone subscriber with that subscriber's express invitation or permission prior to the voice communication.

(ii) A voice communication to an existing customer of the person on whose behalf the voice communication is made, unless the existing customer is a consumer who has requested that he or she not receive calls from or on behalf of that person under section 1c(1)(g).

(iii) A voice communication to a residential telephone subscriber in which the caller requests a face-to-face meeting with the residential telephone subscriber to discuss a purchase, sale, or rental of, or investment in, goods or services but does not urge the residential telephone subscriber to make a decision to purchase, sell, rent, invest, or make a deposit on that good or service during the voice communication.

(n) "Telephone solicitor" means any person doing business in this state who makes or causes to be made a telephone solicitation from within or outside of this state, including, but not limited to, calls made by use of automated dialing and announcing devices or by a live person.

(o) "Vendor" means a person designated by the commission to maintain a do-not-call list under section 1a. The term may include a governmental entity.

Sec. 1a. (1) A home solicitation sale shall not be made by telephonic solicitation using in whole or in part a recorded message. A person shall not make a telephone solicitation that consists in whole or in part of a recorded message.

(2) Within 120 days after the effective date of the amendatory act that added this subsection, the commission shall do 1 of the following:

(a) Establish a state do-not-call list. All of the following apply if the commission establishes a do-not-call list under this subdivision:

(i) The commission shall publish the do-not-call list quarterly for use by telephone solicitors.

(ii) The do-not-call list fund is created in the state treasury. Money received from fees under subparagraph (iii) shall be credited to the fund. The state treasurer shall direct the investment of the fund. The state treasurer shall credit to the fund interest and earnings from fund investments. Money remaining in the fund at the end of a fiscal year shall be carried over in the fund to the next and succeeding fiscal years. Money in the fund may be appropriated to the commission to cover the costs of administering the do-not-call list, but may not be appropriated to compensate or reimburse a vendor designated under subdivision (b) to maintain a do-not-call list under that subdivision.

(iii) The commission shall establish and collect 1 or both of the following fees to cover the costs to the commission for administering the do-not-call list:

(A) Fees charged to telephone solicitors for access to the do-not-call list.

(B) Fees charged to residential telephone subscribers for inclusion on the do-not-call list. The commission shall not charge a residential telephone subscriber a fee of more than $ 5.00 for a 3-year period.

(iv) The commission shall maintain the do-not-call list for at least 1 year. After 1 year, the commission may at any time elect to designate a vendor to maintain a do-not-call list under subdivision (b), in which case subdivision (b) shall apply.

(b) Designate a vendor to maintain a do-not-call list. All of the following apply to a vendor designated to maintain a do-not-call list under this subdivision:

(i) The commission shall establish a procedure or follow existing procedure for the submission of bids by vendors to maintain a do-not-call list under this subdivision.

(ii) The commission shall establish a procedure or follow existing procedure for the selection of the vendor to maintain the do-not-call list. In selecting the vendor, the commission shall consider at least all of the following factors:

(A) The cost of obtaining and the accessibility and frequency of publication of the do-not-call list to telephone solicitors.

(B) The cost and ease of registration on the do-not-call list to consumers who are seeking inclusion on the do-not-call list.

(iii) The commission may review its designation and make a different designation under this subdivision if the commission determines that another person would be better than the designated vendor in meeting the selection factors established under subparagraph (ii) or if the designated vendor engages in activities the commission considers contrary to the public interest.

(iv) If the commission does not establish a state do-not-call list under subdivision (a), the commission shall comply with the designation requirements of this subdivision for at least 1 year. After 1 year, the commission may at any time elect to establish and maintain a do-not-call list under subdivision (a), in which case subdivision (a) shall apply.

(v) Unless the vendor is a governmental entity, a vendor designated by the commission under this subdivision is not a governmental agency and is not an agent of the commission in maintaining a do-not-call list.

(vi) The commission and a vendor designated under this subdivision shall execute a written contract. The contract shall include the vendor's agreement to the requirements of this section and any additional requirements established by the commission.

(vii) The commission shall not use state funds to compensate or reimburse a vendor designated under this subdivision. The vendor may receive compensation or reimbursement for maintaining a designated do-not-call list under this subdivision only from 1 or both of the following:

(A) Fees charged by the vendor to telephone solicitors for access to the do-not-call list.

(B) Fees charged by the vendor to residential telephone subscribers for inclusion on the do-not-call list. A designated vendor shall not charge a residential telephone subscriber a fee of more than $ 5.00 for a 3-year period.

(viii) The designee do-not-call list fund is created in the state treasury. If the vendor is a department or agency of this state, money received from fees under subparagraph (vii) by that vendor shall be credited to the fund. The state treasurer shall direct the investment of the fund. The state treasurer shall credit to the fund interest and earnings from fund investments. Money remaining in the fund at the end of a fiscal year shall be carried over in the fund to the next and succeeding fiscal years. Money in the fund may be appropriated to that vendor to cover the costs of administering the do-not-call list.

(3) In determining whether to establish a state do-not-call list under subsection (2)(a) or designate a vendor under subsection (2)(b), and in designating a vendor under subsection (2)(b), the commission shall consider comments submitted to the commission from consumers, telephone solicitors, or any other person.

(4) Beginning 90 days after the commission establishes a do-not-call list under subsection (2)(a) or designates a vendor to maintain a do-not-call list under subsection (2)(b), a telephone solicitor shall not make a telephone solicitation to a residential telephone subscriber whose name and residential telephone number is on the then-current version of that do-not-call list.

(5) Notwithstanding any other provision of this section, if an agency of the federal government establishes a federal do-not-call list, within 120 days after the establishment of the federal do-not-call list, the commission shall designate the federal list as the state do-not-call list. The federal list shall remain the state do-not-call list as long as the federal list is maintained. A telephone solicitor shall not make a telephone solicitation to a residential telephone subscriber whose name and residential telephone number is on the then-current version of the federal list.

(6) A telephone solicitor shall not use a do-not-call list for any purpose other than meeting the requirements of subsection (4) or (5).

(7) The commission or a vendor shall not sell or transfer the do-not-call list to any person for any purpose unrelated to this section.

Sec. 1b. (1) At the beginning of a telephone solicitation, a person making a telephone solicitation to a residential telephone subscriber shall state his or her name and the full name of the organization or other person on whose behalf the call was initiated and provide a telephone number of the organization or other person on request. A natural person must be available to answer the telephone number at any time when telephone solicitations are being made.

(2) The person answering the telephone number required under subsection (1) shall provide a residential telephone subscriber calling the telephone number with information describing the organization or other person on whose behalf the telephone solicitation was made to the residential telephone subscriber and describing the telephone solicitation.

(3) A telephone solicitor shall not intentionally block or otherwise interfere with the caller ID function on the telephone of a residential telephone subscriber to whom a telephone solicitation is made so that the telephone number of the caller is not displayed on the telephone of the residential telephone subscriber.

Sec. 1c. (1) It is an unfair or deceptive act or practice and a violation of this act for a telephone solicitor to do any of the following:

(a) Misrepresent or fail to disclose, in a clear, conspicuous, and intelligible manner and before payment is received from the consumer, all of the following information:

(i) Total purchase price to the consumer of the goods or services to be received.

(ii) Any restrictions, limitations, or conditions to purchase or to use the goods or services that are the subject of an offer to sell goods or services.

(iii) Any material term or condition of the seller's refund, cancellation, or exchange policy, including a consumer's right to cancel a home solicitation sale under section 2 and, if applicable, that the seller does not have a refund, cancellation, or exchange policy.

(iv) Any material costs or conditions related to receiving a prize, including the odds of winning the prize, and if the odds are not calculable in advance, the factors used in calculating the odds, the nature and value of a prize, that no purchase is necessary to win the prize, and the "no purchase required" method of entering the contest.

(v) Any material aspect of an investment opportunity the seller is offering, including, but not limited to, risk, liquidity, earnings potential, market value, and profitability.

(vi) The quantity and any material aspect of the quality or basic characteristics of any goods or services offered.

(vii) The right to cancel a sale under this act, if any.

(b) Misrepresent any material aspect of the quality or basic characteristics of any goods or services offered.

(c) Make a false or misleading statement with the purpose of inducing a consumer to pay for goods or services.

(d) Request or accept payment from a consumer or make or submit any charge to the consumer's credit or bank account before the telephone solicitor or seller receives from the consumer an express verifiable authorization. As used in this subdivision, "verifiable authorization" means a written authorization or confirmation, an oral authorization recorded by the telephone solicitor, or confirmation through an independent third party.

(e) Offer to a consumer in this state a prize promotion in which a purchase or payment is necessary to obtain the prize.

(f) Fail to comply with the requirements of section 1a or 1b.

(g) Make a telephone solicitation to a consumer in this state who has requested that he or she not receive calls from the organization or other person on whose behalf the telephone solicitation is made.

(2) Except as provided in this subsection, beginning 210 days after the effective date of the amendatory act that added this section, a person who knowingly or intentionally violates this section is guilty of a misdemeanor punishable by imprisonment for not more than 6 months or a fine of not more than $ 500.00, or both. This subsection does not prohibit a person from being charged with, convicted of, or punished for any other crime including any other violation of law arising out of the same transaction as the violation of this section. This subsection does not apply if the violation of this section is a failure to comply with the requirements of section 1a(1), (4), or (5) or section 1b.

(3) A person who suffers loss as a result of violation of this section may bring an action to recover actual damages or $ 250.00, whichever is greater, together with reasonable attorney fees. This subsection does not prevent the consumer from asserting his or her rights under this act if the telephone solicitation results in a home solicitation sale, or asserting any other rights or claims the consumer may have under applicable state or federal law.

Sec. 1d. (1) Beginning 210 days after the effective date of the amendatory act that added this section, if a telephone directory includes residential telephone numbers, a person that publishes a new telephone directory shall include in the telephone directory a notice describing the do-not-call list and how to enroll on the do-not-call list.

(2) Beginning 210 days after the effective date of the amendatory act that added this section, each telecommunication provider that provides residential telephone service shall include a notice describing the do-not-call list and how to enroll on the do-not-call list with 1 of that telecommunication provider's bills for telecommunication services to a residential telephone subscriber each year. If the federal communication commission or any other federal agency establishes a federal "do not call" list, the notice shall also describe that list and how to enroll on that list. As used in this subsection, "telecommunication provider" means that term as defined in section 102 of the Michigan telecommunications act, *1991 PA 179*, MCL 484.2102.

Sec. 1e. Sections 1a, 1b, 1c, and 1d do not apply to a person subject to any of the following:

(a) The charitable organizations and solicitations act, *1975 PA 169*, MCL 400.271 to 400.294.

(b) The public safety solicitation act, *1992 PA 298*, MCL 14.301 to 14.327.

(c) Section 527 of the internal revenue code of 1986.

Sec. 3. (1) In a home solicitation sale, unless the buyer requests the seller to provide goods or services without delay in an emergency, the seller shall present to the buyer and obtain the buyer's signature to a written agreement or offer to purchase that designates as the date of the transaction the date on which the buyer actually signs. The agreement or offer to purchase shall contain a statement substantially as follows in immediate proximity to the space reserved in the agreement or offer to purchase for the signature of the buyer:

"You, the buyer, may cancel this transaction at any time prior to midnight of the third business day after the date of this transaction. See the attached notice of cancellation form for an explanation of this right. Additionally, the seller is prohibited from having an independent courier service or other third party pick up your payment at your residence before the end of the 3-business-day period in which you can cancel the transaction."

(2) The seller shall attach to the copy or cause to be printed on the reverse side of the written agreement or offer to purchase retained by the buyer a notice of cancellation in duplicate that shall appear as follows: "notice of cancellation (enter date of transaction) (date) You may cancel this transaction, without any penalty or obligation, within 3 business days from the above date. If you cancel, any property traded in, any payments made by you under the contract or sale, and any negotiable instrument executed by you will be returned within 10 business days following receipt by the seller of your cancellation notice, and any security interest arising out of the transaction will be canceled. If you cancel, you must make available to the seller at your residence, in substantially as good condition as when received, any goods delivered to you under this contract or sale; or you may if you wish, comply with the instructions of the seller regarding the return shipment of the goods at the seller's expense and risk. If you do make the goods available to the seller and the seller does not pick them up within 20 days of the date of your notice of cancellation, you may retain or dispose of the goods without any further obligation. If you fail to make the goods available to the seller or if you agree to return the goods to the seller and fail to do so, then you remain liable for performance of all obligations under the contract. To cancel this transaction, mail or deliver a signed and dated copy of this cancellation notice or any other written notice, or send a telegram to (name of seller), at (address of seller's place of business) not later than midnight on _____ (date) I hereby cancel this transaction. _____ (date) _____ (buyer's signature) "

(3) The notices required by this section shall be in not less than 10-point bold type and shall be 2 points larger than the text of the contract. A written agreement or offer to purchase and the notice of cancellation attached to the agreement or offer shall be written in the same language as that used in any oral presentation that was given to facilitate sale of the goods or services. The seller shall enter on the blanks in the notice of cancellation the date of transaction, which is the date the buyer signs the written agreement, and the date for mailing the notice of cancellation. An error in entering this information shall not diminish the buyer's rights under this act.

(4) Until the seller has complied with this section, the buyer may cancel the home solicitation sale by notifying the seller in any manner and by any means of his or her intention to cancel.

(5) This section does not apply to a home solicitation sale where the seller engaged in a telephone solicitation of the sale if sections 505 to 507 of the Michigan telecommunications act, *1991 PA 179*, MCL 484.2505 to 484.2507, apply to the solicitation or sale.

Sec. 6. In connection with a home solicitation sale, refunds or penalties to which the debtor is entitled pursuant to this act may be set off against the debtor's obligation, and may be raised as a defense to an action on the obligation without regard to the time limitations prescribed by this act.

HISTORY:

Approved by the Governor on December 20, 2002

SPONSOR: Faunce