



11490 HOUSE JUDICIARY

HB

308

FISCAL NOTE

STATE OF ALASKA
2006 LEGISLATIVE SESSION

Fiscal Note Number: _____
 Bill Version: HB308-Courts-3-17-08
 () Publish Date: _____

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 3/17/08 @ 10:30 am
 Approved by: Doug Wooliver for Stephanie Cole, Administrative Director Date 3/17/2008
 Agency: Alaska Court System

FISCAL NOTE

STATE OF ALASKA
2006 LEGISLATIVE SESSION

Fiscal Note Number: _____
 Bill Version: HB 308
 () Publin Date: _____

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

FISCAL NOTE

STATE OF ALASKA
2006 LEGISLATIVE SESSION

Fiscal Note Number: _____
 Bill Version: HE306-DPS-AST-3-17-06
 () Publish Date: _____

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 Helms 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

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 9801-1182

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

HB308

An Act relating to false caller identification

Warning. Do not trust your telephone caller ID. The name and number you see may be fake. Both private individuals and commercial spoofer can now deliberately cause false caller identification to be displayed on your caller ID screen. False caller identification is more serious than pranks, or the annoyance of intrusive telemarketing. It facilitates fraud, and can be potentially deadly.

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. Seniors could be victimized by scam artists who appear to be phoning from a reputable agency. 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 lure women and children for purposes of sexual assault or murder. The potential of false caller ID spoofing for crime and other mischief is almost endless.

Anyone with sufficient computer and telephonic skills can implement false caller identification. In fact an entire telephone spoofing industry has emerged, and is growing daily. Cost from one company for spoof calls is 10 cents a minute. These spoofing services can work with mobile phones, landlines as well as telephone services that are routed via the Internet.

The fake caller ID situation is primarily a federal issue, but it is essential that Alaska take whatever action possible within its jurisdiction. Caller ID spoofing from a local, state, or federal law enforcement agency is excluded from this bill.

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

1 **"An Act relating to false caller identification."**

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

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

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

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

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

10 (d) In this section,

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

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

1
2
3
4
5

(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:

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



 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."

All rights reserved. Users may download and print extracts of content from this website for their own personal and non-commercial use only. Republication or redistribution of Reuters content, including by framing or similar means, is expressly prohibited without the prior written consent of Reuters. Reuters and the Reuters sphere logo are registered trademarks or trademarks of the Reuters group of companies around the world.

© Reuters 2005

Close This Window



News & Information for Contact Center Professionals

FIND:

WHITE PAPER



Contact Center Today

February 7, 2006
Updated Daily

Contact Center Today ▾

- Home
- Channel Management
- CSR Management
- Real-Time Analytics
- Systems and Apps
- Voice over IP (VoIP)
- Outsourcing
- CIO Today Magazine

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-ID opens the door to a variety of abuses. "What an appallingly bad id security firm Sophos.

Top Tech News ▾

- Home
- Hardware
- Software
- World Wide Web
- Personal Technology
- Tech Trends
- Science
- Product Reviews
- Business Briefing for Geeks

advertisement!

Reports tell you what has happened in the past. Forecasts tell you what might happen in you what is happening right now. Learn how to gain insight into your current operations. and Agility: Event Stream Processing for Event-Driven Business"

>> 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.

- CIO Today ▾
- Home/CIO News
- CIO Interviews
- Business Briefing
- E-Business
- Infrastructure
- Integration
- Customer Relations
- Data Storage
- Network Security
- Wireless Internet
- Small Business
- Worldwide Tech
- Science & Innovation
- Web Services
- Compliance

Free Newsletters

Top CIO News

Contact Center Industry Alert

your email

sign up

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.

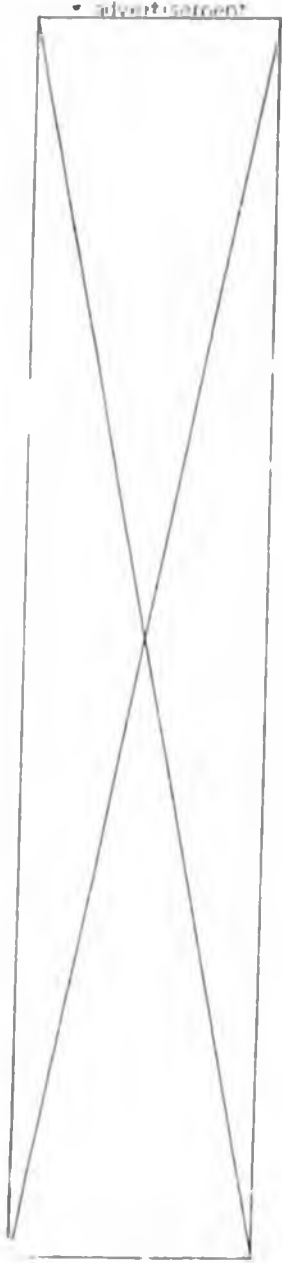
Collection agencies, though, have not entirely shed their less-than-upstanding practices since the passage of the Fair Debt Collection Practices Act. Recently, one firm was fined for continually contacting and harassing a debtor's neighbors -- a

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



Most Popular Article

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 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.

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 to Biggest I.T. Outsourcing](#)
- [Is On-Demand CRM Rig](#)
- [Another Look at Outsour](#)
- [VoIP Conversion Gather](#)

Sponsored Links

- [See what's possible at Avaya Virtual Technology Summit, March 9.](#)
- [The HP ProLiant ML110 G3 server with Intel® Pentium® 4 Processor.](#)
- [SAN Connectivity in Virtualized Server Environments from Emulex](#)
- [Progress® Apama® lets you gain insight into your current operations.](#)
- [DualPath Outdoor Wireless Bridges. Get online price estimates.](#)
- [Special 2 for 1 Offer & Free IDC Virtualization White Paper from HP.](#)
- [3Com's TippingPoint™ IPS: Plug it in.](#)
- [Windows Server vs. Linux SuSE: Read the Security Innovation study.](#)
- [Best in class enterprise IT solutions from 3Com](#)



FUTURE TENSE[®]

WITH JON GORDON

Search Future Tense

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 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			

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 security threat

problem like e-mail spoofing.

"If you pick up your 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 spoofing, 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 EASE Actually, 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 SPOOFERThe 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.



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 officer 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>

Copyright © 1999-2005 SecurityFocus

T-Mobile security flaw in voicemail. Beware and change



By **David Liccone**, 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?... Cover 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 whcever 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!

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 VertCall 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 greeting. (not what ever you recorded) You could then interrupt to say hi after confirming it was actually someone 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

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.

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 prank last 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 a 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 mentioned 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 Daniele 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 Carnophone.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 FDCPA.

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 FDCPA. 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 FDCPA," 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](#)

EMAIL THIS ARTICLE 
PRINT THIS ARTICLE 
DISCUSS THIS ARTICLE 
WRITE TO AN EDITOR 

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 reached.

WHITEPAPERS & WEBCASTS

FISCAL NOTE

STATE OF ALASKA
2006 LEGISLATIVE SESSION

Fiscal Note Number: _____
 Bill Version: HB308-Courts-3-17-06
 () Publish Date: _____

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, Administrative Director Date 3/17/2006
 Agency Alaska Court System

FISCAL NOTE

STATE OF ALASKA
2006 LEGISLATIVE SESSION

Fiscal Note Number: _____
 Bill Version: HB 308
 () Publish Date: _____

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
 Division: Public Defender Agency
 Approved by: Mike Tibbles, Deputy Commissioner
 Agency: Administration

Phone (907) 334-4414
 Date/Time 3/21/06 9:06 a.m.
 Date 3/21/2006

FISCAL NOTE

STATE OF ALASKA
2006 LEGISLATIVE SESSION

Fiscal Note Number: _____
 Bill Version: HB308-DPS-AST-3-17-06
 () Publish Date: _____

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

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

March 23, 2006

Congressman Murphy
322 Cannon House Office Building
Washington DC 20515

Dear Congressman Murphy:

We are looking forward to your teleconference testimony on Alaska HB308, especially as someone who has been personally victimized by Caller ID spoofing. The fact that you are an elected official, who suffered personal damage from Caller ID spoofing, communicating to the elected officials on our Judiciary Committee should be very helpful.

The Alaska House Judiciary Committee hearing on HB308 has been rescheduled to Wednesday, March 29th, 2006 at 5:00PM Eastern Standard Time. My staff will assist you with the teleconference call-in number.

Also, in your dealing with the Caller ID spoofing situation, please let us know if you are aware of any other resources that could be made available to the Judiciary Committee to help them understand the need for HB308.

Thank you in advance for your help.

Yours truly,

A handwritten signature in black ink that reads "Bob Lynn". The signature is fluid and cursive, with a long horizontal stroke extending to the right.

Representative Bob Lynn

cc: Lesil McGuire, Chair
House Judiciary Committee



CONGRESSMAN

Tim Murphy

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 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 ten 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.

Biography

About The District

Test Room

Home

Media

Constituent Services

Photo Gallery

Contact Tim

District Links

Visit Washington DC

Email Updates

Your Email Address

Subscribe





CONGRESSMAN Tim Murphy



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](#)

- Home
- About The District
- Biography
- Issues
- Multi-Media
- Constituent Services
- Photo Gallery
- Contact Tim
- District Links
- Visit Washington DC
- Email Updates

Your Email Address

Subscribe



[Home](#) | [Biography](#) | [About The District](#) | [NewsRoom](#) | [Issues](#) | [Constituent Services](#) | [Photo Gallery](#)
[Contact Tim](#) | [District Links](#) | [Visit Washington DC](#) | [Kid's Page](#) | [Privacy Policy](#)

HOME > BUSINESS > TECHNOLOGY

ADVERTISEMENT

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



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, [Spooftcard.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 Jarnes, 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, [Spooftcard.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 [Spooftcard.com](#) and [Spooftel.com](#) say they will surrender call logs to authorities in response to subpoenas. [Spooftcard.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

▶ [Advanced search / Historic Archives](#)

ADVERTISEMENT

Start saving on every call with Vonage.
Sign up now and get 1 FREE month of phone service!
www.vonage.com

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 incoming 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 [Spooftcard.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. ■

© Copyright 2006 Associated Press. All rights reserved. This material may not be published, broadcast, rewritten, or redistributed.

MORE:

[Business section](#) | [Latest business news](#) | [Globe front page](#) | [Boston.com](#)

SIGN UP FOR: [Globe Headlines e-mail](#) | [Breaking News Alerts](#)

FISCAL NOTE

STATE OF ALASKA
2006 LEGISLATIVE SESSION

Fiscal Note Number: _____
 Bill Version: HB308-Courts-3-17-06
 () Publish Date: _____

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, Administrative Director Date 3/17/2006
 Agency: Alaska Court System

FISCAL NOTE

STATE OF ALASKA
2006 LEGISLATIVE SESSION

Fiscal Note Number: _____
 Bill Version: HB 308
 () Publish Date: _____

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

FISCAL NOTE

STATE OF ALASKA
2006 LEGISLATIVE SESSION

Fiscal Note Number: _____
 Bill Version: HB308-DPS-AST-3-17-06
 () Publish Date: _____

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
 Division: Alaska State Troopers
 Approved by: Commissioner William Tandeske
 Agency: Department of Public Safety

Phone 907-269-4532
 Date/Time 3/17/06 1:54 PM
 Date 3/17/2006

HB

314

ALASKA STATE HOUSE OF REPRESENTATIVES



Session

(907)-465-3719

FAX# (907)-465-3258

State Capitol
Room 204

Contact:

Interim Address:

**3340 Badger Road
North Pole, AK 99705
(907)-488-5725
Fax# (907)-488-4271**

REPRESENTATIVE JOHN COGHILL

HB 314 "No Retreat Defense"

SPONSOR STATEMENT

This legislation came to my attention when Florida passed similar legislation last year. but was brought closer to home when a man in Wasilla was shot after being chased out of his own home by an intruder.

Unlike Florida, Alaska law allows a person to use deadly force in defense of death, serious physical injury, kidnapping, sexual assault or robbery in their home. HB 314 broadens the law to include any place a person has a right to be.

If a person fears for their life or is under attack, they should be able to stand their ground whether in their home, or the parking lot of the local grocery store.

Sexual assault is no longer about promiscuity, but physical mangling, kidnapping, rape and, too often, death. HB 314 allows a person to use deadly force when protecting a child from sexual assault.

This bill addresses defense from car jacking. A person may use deadly force from inside or outside the vehicle to terminate a car jacking.

This legislation also provides immunity from civil liability against people that use deadly force to defend themselves. I don't believe there was ever an intention of this being able to happen to a law abiding person just trying to defend themselves.

Those who intend to do bodily harm, kidnap, or sexually assault another person should "beware." This bill empowers people to defend themselves and others. You can't blow a whistle and expect the police to show up; I say stand your ground.

ALASKA STATE HOUSE OF REPRESENTATIVES



Session

Contact:

Interim Address:

3340 Badger Road
North Pole, AK 99705
(907)-488-5725
Fax# (907)-488-4271

(907)-465-3719
FAX# (907)-465-3258
State Capitol
Room 204

REPRESENTATIVE JOHN COGHILL

HB 314 - No Retreat Defense

SECTIONAL

Section 1

HB 314 amends the Code of Civil Procedure, Title 9, by adding immunity from civil liability against a person that uses force, unless it is against a peace officer engaged in the performance of official duties, identified as a peace officer, or reasonably known as a peace officer.

This section also provides for reasonable attorney fees, court, costs, compensation for loss of income, and all expenses incurred as a result of such a civil action.

Section 2

Under current law a person can use deadly force if it is a situation that allows non-deadly force and the person believes deadly force is needed for self-defense against death, serious injury, kidnapping, sexual assault, and robbery in any degree.

Section 2(a) adds sexual abuse of a minor as a reason to defend the minor with the use deadly force.

No duty to retreat already applies in Alaska on premises a person owns or leases. Section 2 (b) is amended in HB 314 and expands "no retreat" to any place a person has a right to be.

Section 3

Provides that deadly force can be used and no retreat has to be made to protect a child from imminent threat of death, serious physical injury, kidnapping, sexual assault, sexual abuse of a minor, or robbery.

Section 4

Provides that a person inside or outside a vehicle may use deadly force if necessary to terminate a carjacking or theft of a vehicle when someone other than the offender is inside the vehicle.

HB

316

ALASKA STATE LEGISLATURE

Chair:
House Finance Subcommittees for,
Department of Public Safety
Department of Law

Member:
House Finance Committee
Legislative Council



Session:
Alaska State Capitol
Juneau, AK 99801-1182
Phone: (907) 465-4958
Fax: (907) 465-4928

Interim:
PO Box 464
Chugak, AK 99567

REPRESENTATIVE BILL STOLTZE

Representative_Bill_Stoltze@legis.state.ak.us

MEMORANDUM

TO: Representative Lesil McGuire, Chair
House Judiciary Committee

FROM: Representative Bill Stoltze *BS*

DATE: April 12, 2006

SUBJECT: Hearing Request

I respectfully request a hearing be scheduled for House Bill 316, an Act extending the termination date for the Board of Governors of the Alaska Bar Association.

Thank you for your consideration.

DISRICT 16

BIRCHWOOD • BUTTE • CHUGIAK • EKLUTNA • FAIRVIEW LOOP
KNIK RIVER ROAD • LAZY MOUNTAIN • PALMER • PETERS CREEK

ALASKA STATE LEGISLATURE

Vice Chair:
House Finance Committee

Chair:
House Finance Subcommittees for,
Department of Public Safety
Department of Law



Session:
Alaska State Capitol
Juneau, AK 99801-1182
Phone: (907) 465-4958
Fax: (907) 465-4928

Interim:
PO Box 464
Chugak, AK 99567

BILL STOLTZE **STATE REPRESENTATIVE**

Representative_Bill_Stoltze@legis.state.ak.us

House Bill 316

Extend the Termination Date for the Board of Governors ABA

"An act extending the termination date for the Board of Governors of the Alaska Bar Association; and providing for an effective date."

House Bill 316 extends the sunset date of the Board of Governors of the Alaska Bar Association until June 30, 2009.

The Board of Governors for the Alaska Bar Association is comprised of 12 members. Nine members are elected by active members of the Alaska Bar Association: two from the 1st judicial district, four from the 3rd judicial district, two from the 2nd/4th judicial districts, and one at-large member. There are also three non-attorney members appointed by the Governor and confirmed by the Legislature. The Board governs the Bar Association, administers exams, approves and recommends rules concerning practice of law to the State Supreme Court, and provides continuing legal education and member services.

It is the opinion of the Legislative Budget and Audit Committee that the Board of Governors of the Alaska Bar Association should be extended. I ask your support in extended its sunset date to June 30, 2009.

DISTRICT 16

BIRCHWOOD • BUTTE • CHUGIAK • EKLUTNA • FAIRVIEW LOOP
KNIK RIVER ROAD • LAZY MOUNTAIN • PALMER • PETERS CREEK

HB

318

Alaska State Legislature

House of Representatives



Official Business

State Capitol
Juneau, AK 99801-1182

SPONSOR STATEMENT FOR HB 150

BY: Representative Tom Anderson

"An Act requiring licensure of occupations relating to radiologic technology, radiation therapy, and nuclear medicine technology; and providing for an effective date."

The Radiologic Health Science professionals in the State of Alaska are dedicated to the preservation of life and health as well as the prevention and treatment of disease. The use of x-rays and other medical imaging disciplines is the most acceptable method for discovering and treating many conditions that might not otherwise be observed until it is too late for treatment.

The unregulated practice of Radiologic Technology, Nuclear Medicine Technology and Radiation Therapy by unqualified individuals represents a serious health risk to the citizens of Alaska. The Alaska Society of Radiologic Technologists has consistently supported the enactment of state standards for the education and credentialing of Radiologic Technologists, Radiation Therapists and Nuclear Medicine Technologists as a means of protecting Alaskans from the harmful effects of excessive and unnecessary exposure to medical radiation.

Any radiology procedure is only as effective as the person performing it. An underexposed chest x-ray cannot reveal pneumonia or a malignant lesion, just as an inadequate mammography technique cannot detect breast cancer. No matter what the procedure, the Radiologic Technologist's knowledge of anatomy, careful application of radiation and skillful operation of sophisticated medical equipment are the keys to its success. Patients have long benefited from Alaska's wisely implemented Radiology equipment performance standards but those benefits can easily be negated by under trained operators of the equipment. To be clinically useful, diagnostic imaging exams must be accurate. To stop invasive cancers, radiation therapy treatments must be precise.

To ensure that the citizens of the State of Alaska receive maximum protection practicable from the harmful effects of excessive and improper exposure to ionizing radiation, licensure must be passed to establish standards.

Establishing state standards will ensure that Alaskans will have access to safe and high quality radiologic care. Licensure for Radiologic Technologists, Radiation Therapists and Nuclear Medicine Technologists will establish radiation protection measures as well as education and credentialing standards that will ensure the competency of persons operating medical equipment emitting radiation.

I urge your support of this important piece of legislation.

24-LS0470\R

Alaska State Legislature

House of Representatives



Official Business

State Capitol
Juneau, AK 99801-1182

Sectional Analysis for HB 150 BY: Representative Tom Anderson

Section 1. Amends AS 08 is amended to add a new section

Sec. 08.89.100 defines who needs to acquire a Radiological Technician license under this bill. Also provides exemptions for the license.

Sec. 08.89.110 limits the titles a person can use if they do not hold a license.

Sec. 08.89.120 defines the minimum requirements to receive a license

Sec. 08.89.130 describes how the Department of Health and Social Services shall approve licensure programs.

Sec. 08.89.140 describes the radiological licensure examinations.

Sec. 08.89.150 defines the qualifications for a limited radiological imager license

Sec. 08.89.160 describes how the Department of Health and Social Services shall approve limited radiological licensure programs.

Sec. 08.89.170 provides for the application and scope of a temporary permit for practice of radiology and allows a person to receive such a permit if they can prove they were performing radiological work before the passage of HB 150

Sec. 08.89.180 defines the license renewal process

Sec. 08.89.190 states that a licensee must keep their license or a copy of their license on file at their place of employment

Sec. 08.89.200 states that the licensee must notify the Department of a name or address change within 30 days

Sec. 08.89.210 states that a person whose license is revoked for a reason other than late payment of fees must wait 24 months before reapplying for a license.

Sec. 08.89.220 directs the Department to set fees for various aspect of the licensure process.

Sec. 08.89.300 limits the use of radiological equipment on a patient without a prescription.

Sec. 08.89.310 defines a civil penalty for practicing radiology without a license.

Sec. 08.89.320 defines a criminal penalty for a person who obtains or attempts to obtain a license through fraudulent means.

Sec.08.89.330 defines the grounds for disciplinary actions or denial of license.

Sec. 08.89.340 defines under what situations the Department may impose sanctions on a licensee.

Sec. 08.89.900 states that for the purposes of 08.01.065, all persons who hold a radiological license are considered to be engaged in the same occupation.

Sec. 08.89.990 outlines various definitions for terms in HB 150.

Section 2. Amends AS 44.64.030(a)(6)

This allows the Board of Radiological Technicians to conduct disciplinary hearings.

Section 3. The uncodified law of the State of Alaska is amended

Directs the Department of Commerce, Community and Economic Development and the division of occupational licensing to begin the process of adopting and implementing the regulations created by HB 150.

Section 4. The uncodified law of the State of Alaska is amended

Details revisors' instructions for reconciliation of sec. 2 of this bill with sec. 82, ch. 163, SLA 2004.

Section 5 Effective date of this act except as provided by sec. 6 and 7

Section 6. Effective date of AS 08.89.100 and AS 08.89.310

Section 7. Effective date of Section 3

24-LS0470\R
Mischel
1/12/06

CS FOR HOUSE BILL NO. 150()

**IN THE LEGISLATURE OF THE STATE OF ALASKA
TWENTY-FOURTH LEGISLATURE - SECOND SESSION**

BY

Offered:

Referred:

Sponsor(s): REPRESENTATIVE ANDERSON

A BILL

FOR AN ACT ENTITLED

1 **"An Act requiring licensure of occupations relating to radiologic technology, radiation**
2 **therapy, and nuclear medicine technology; and providing for an effective date."**

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

4 *** Section 1.** AS 08.01.010 is amended by adding a new paragraph to read:

5 (39) regulation of radiographers under AS 08.89.

6 *** Sec. 2.** AS 08 is amended by adding a new chapter to read:

7 **Chapter 89. Radiographers.**

8 **Article 1. Licensing Requirements.**

9 **Sec. 08.89.100. Unlicensed practice prohibited.** (a) Except as provided in (b)
10 of this section, a person may not knowingly

11 (1) use radioactive materials or equipment emitting radiation on a
12 human for diagnostic or therapeutic purposes without a license or permit issued under
13 this chapter that authorizes the person to do so; or

14 (2) employ another to use radioactive materials or equipment emitting

1 radiation on a human for diagnostic or therapeutic purposes unless the employee has
2 an appropriate license or permit issued under this chapter.

3 (b) The licensing or permit requirement in (a) of this section does not apply to
4 a person who is

5 (1) a licensed practitioner;

6 (2) a dental assistant who uses equipment emitting radiation on
7 humans under the supervision of a licensed practitioner;

8 (3) licensed under another provision of state law if the license
9 authorizes the person to use radioactive materials or equipment emitting radiation on a
10 human for diagnostic or therapeutic purposes; or

11 (4) a student enrolled in and attending a school or college of medicine,
12 osteopathy, dentistry, dental hygiene, chiropractic, podiatry, radiologic technology,
13 radiation therapy, or nuclear medicine, while, as part of course work in the school or
14 college, the student uses radioactive materials or equipment emitting radiation on
15 humans under

16 (A) the direct supervision of a licensed practitioner; or

17 (B) the direct supervision of a person fully licensed under this
18 chapter as a radiographer, radiation therapist, or nuclear medicine technologist,
19 as appropriate to the course.

20 (c) Violation of this section is a class A misdemeanor.

21 **Sec. 08.89.110. Use of title prohibited.** (a) Unless a person holds the
22 corresponding full or limited certificate of licensure or permit issued under this
23 chapter or proof of certification by the American Registry of Radiologic Technologists
24 or the Nuclear Medicine Technology Certification Board, a person may not use

25 (1) the title "radiographer," "radiation therapist," "nuclear medicine
26 technologist," "limited radiologic imager," "temporary permitted radiographer,"
27 "temporary permitted radiation therapist," "temporary permitted nuclear medicine
28 technologist," or "temporary permitted limited radiologic imager";

29 (2) an abbreviation that corresponds to a title listed in (1) of this
30 subsection; or

31 (3) another title, abbreviation, letters, figures, signs, or other devices

1 that would lead a reasonable person to believe that the person is licensed or permitted
2 under this chapter.

3 (b) Violation of this section is a class A misdemeanor.

4 **Sec. 08.89.120. Qualifications for full certificate licensure.** (a) In order to
5 receive a full certificate of licensure under this chapter, a person must apply to the
6 department in a manner that indicates whether the person is applying to practice as a
7 radiographer, radiation therapist, or nuclear medicine technologist. In addition, the
8 person shall

9 (1) be at least 18 years of age;

10 (2) have graduated from secondary school or have passed an approved
11 equivalency test;

12 (3) have graduated from a program approved by the department under
13 AS 08.89.130 in the area of practice for which the person seeks licensure;

14 (4) have met the examination requirement under AS 08.89.140 for the
15 area of practice for which the person seeks licensure; and

16 (5) pay the required fees.

17 (b) A full certificate shall specify the area of practice authorized under it.

18 (c) A person with a full certificate of licensure may practice in the authorized
19 area of practice only under the direction of a licensed practitioner.

20 **Sec. 08.89.130. Program approval; full certificates.** (a) The department
21 shall, upon application by a program, evaluate an educational program that trains
22 persons to receive full certificates of licensure under this chapter and approve or
23 disapprove the program according to the criteria in (b) of this section.

24 (b) The department shall approve a program evaluated under this section only
25 if

26 (1) the program is affiliated with at least one hospital that provides a
27 clinical component for the program that is considered to be adequate by the
28 department;

29 (2) the program's curriculum for each course of study in the areas of
30 practice licensed under AS 08.89.120 meets the standards approved by the Joint
31 Review Committee on Education in Radiologic Technology, the Joint Review

1 Committee on Educational Programs in Nuclear Medicine Technology, the United
2 States Department of Education, or another appropriate accreditation agency whose
3 standards are considered equivalent by the department; and

4 (3) a recognized national voluntary accrediting organization has
5 reviewed the program's application to the department and submitted the review
6 comments to the department.

7 **Sec. 08.89.140. Examinations; full certificates.** The examination requirement
8 under AS 08.89.120 may be met by meeting one of the following criteria:

9 (1) successfully passing an examination approved by the department in
10 the area of practice for which the full certificate of licensure is sought;

11 (2) proof of current certification by the American Registry of
12 Radiologic Technologists, Nuclear Medicine Technology Certification Board; or

13 (3) proof of current licensure in the area of practice for which a full
14 certificate of licensure is sought by another jurisdiction with standards for licensure
15 considered by the department to be equivalent to the standards of this state.

16 **Sec. 08.89.150. Qualifications for limited radiologic imager.** (a) In order to
17 be licensed as a limited radiologic imager, a person must

18 (1) be at least 18 years of age;

19 (2) have graduated from secondary school or have passed an approved
20 equivalency test;

21 (3) have graduated from a program approved by the department under
22 AS 08.89.160 or have demonstrated experience sufficient in the opinion of the
23 department to waive the program;

24 (4) have passed the exam approved by the department for limited
25 radiologic imager licensure; and

26 (5) pay the required fees.

27 (b) A limited radiologic imager

28 (1) may perform limited radiologic diagnostic imaging only under the
29 supervision of a fully licensed radiographer or a licensed practitioner;

30 (2) may perform only radiography of the chest, abdomen, and axial-
31 appendicular skeleton;

1 (3) may not perform radiologic procedures involving the use of
2 contrast media, use of fluoroscopic equipment, mammography, tomography, magnetic
3 resonance imaging (MRI), bone densitometry using ionizing radiation, nuclear
4 medicine, radiation therapy, or computed tomography imaging (CT scan).

5 **Sec. 08.89.160. Program approval for limited radiologic imager.** (a) The
6 department shall, upon application by a program, evaluate a program that trains
7 persons to be limited radiologic imagers and approve or disapprove the program
8 according to the criteria in (b) of this section.

9 (b) The department shall approve a program evaluated under this section only
10 if the program includes didactic instruction and clinical instruction considered
11 adequate by the department in axial-appendicular skeleton radiography, chest and
12 abdomen radiography, equipment maintenance and operation, radiation safety and
13 protection, image production and evaluation, radiographic anatomy and positioning
14 procedures, and applicable federal and state requirements relating to patient care and
15 safety; in this subsection, "clinical instruction" means hands-on experience in a health
16 facility setting, such as in a hospital or clinic, under the supervision of a licensed
17 practitioner or fully licensed radiographer.

18 **Sec. 08.89.170. Temporary permit.** (a) The department may issue a
19 nonrenewable temporary

20 (1) limited permit to a person authorizing practice in an area
21 corresponding to the person's scope of radiology training if the person

22 (A) is enrolled in a program for that area approved under
23 AS 08.89.160; and

24 (B) pays the appropriate fee; or

25 (2) full permit to a person authorizing practice in an area
26 corresponding to the person's scope of radiology training if the person

27 (A) has taken an examination described under AS 08.89.140 or
28 08.89.150 for that area and the results are not yet available;

29 (B) applies for the temporary permit within one year after
30 completing a program approved under AS 08.89.130; and

31 (C) pays the appropriate fee.

1 (b) A temporary permit issued under this section must indicate the area of
2 practice authorized. Except as provided in (c) and (d) of this section, the permit
3 expires one year after completion of the program described in (a)(1) of this section or
4 upon receipt of the examination results referred to in (a)(2) of this section, whichever
5 is earlier.

6 (c) Notwithstanding (a) and (b) of this section, the department may issue a
7 nonrenewable temporary permit valid for two years to an applicant who pays a fee
8 determined by the department and who demonstrates to the satisfaction of the
9 department that the applicant has been performing limited scope radiologic diagnostic
10 imaging under AS 08.89.150(b) for two years preceding July 1, 2008. A two-year
11 temporary permit issued under this subsection qualifies the applicant for employment
12 only as specified in AS 08.89.150(b).

13 (d) Notwithstanding (a) - (c) of this section, if an applicant has provided proof
14 of certification by a recognized national credentialing body that covers the area of
15 practice for which a certificate of licensure is sought, the department may issue a
16 nonrenewable temporary permit valid for a period of one year to the applicant upon
17 payment of a fee determined by the department .

18 (e) A person who holds a permit under this section is entitled to use the title
19 "temporary permitted radiographer," "temporary permitted radiation therapist,"
20 "temporary permitted nuclear medicine technologist," or "temporary permitted limited
21 radiologic imager."

22 **Sec. 08.89.180. License renewal; continuing education.** (a) The department
23 may not renew a full certificate of licensure issued under this chapter unless the
24 licensee pays the required fee and submits evidence satisfactory to the department that
25 the person has met the applicable continuing education requirements as determined by
26 the department.

27 (b) A person with a full certificate of licensure who is licensed to practice in
28 more than one area of practice is not required to complete more continuing education
29 than a person with a full certificate of licensure who is licensed in only one area of
30 practice. However, the department, in its communications with persons who have a
31 full certificate of licensure in more than one area of practice, shall encourage those

1 persons to receive continuing education in all of the areas for which they are licensed.

2 (c) The department may not renew a limited radiological imager license issued
3 under this chapter unless the licensee pays the required fee and submits evidence
4 satisfactory to the department that the person has met the applicable continuing
5 competency requirements as determined by the department.

6 **Sec. 08.89.190. License or permit to be kept on file.** A person licensed or
7 holding a permit under this chapter shall keep on file at each place of the person's
8 employment the license or permit document issued under this chapter or a verified
9 copy of the license or permit document.

10 **Sec. 08.89.200. Notification of address changes.** A licensee or permittee
11 under this chapter shall notify the department in writing within 30 days after a name or
12 address change.

13 **Sec. 08.89.210. Reapplication after revocation.** A person whose license or
14 permit is revoked by the department for a reason other than nonpayment of fees may
15 not apply to be licensed under this chapter until one year has elapsed from the date of
16 revocation. The department may require an examination for reinstatement.

17 **Sec. 08.89.220. Fees.** The department shall set fees under AS 08.01.065 for
18 each of the following:

- 19 (1) application;
- 20 (2) examination;
- 21 (3) full certificate of licensure;
- 22 (4) limited certificate of licensure;
- 23 (5) temporary full permit;
- 24 (6) temporary limited permit;
- 25 (7) license renewal;
- 26 (8) adding an area of practice to an existing license;
- 27 (9) program approval under AS 08.89.130.

28 **Article 2. Prohibitions; Penalties; Disciplinary Sanctions.**

29 **Sec. 08.89.300. Prescription required.** (a) A person holding a license or
30 permit issued under this chapter may not knowingly use a radioactive substance or
31 equipment for radiologic procedures on a human for diagnostic or therapeutic

1 purposes except as prescribed by a licensed practitioner.

2 (b) Violation of this section is a class A misdemeanor.

3 **Sec. 08.89.310. Civil penalty for unlicensed practice.** A person required to
4 be licensed or to have a permit under this chapter who engages or offers to engage in a
5 type of diagnostic radiologic imaging, radiation therapy, or nuclear medicine
6 technology for which the person is not licensed or for which the person does not hold
7 a permit may be fined up to \$5,000 under the citation procedures of AS 08.01.102 -
8 08.01.104.

9 **Sec. 08.89.320. Criminal penalty for certain fraudulent practices.** A person
10 who obtains or attempts to obtain a license or permit under this chapter by dishonest or
11 fraudulent means or who knowingly forges, counterfeits, or fraudulently alters a
12 license or permit issued under this chapter is guilty of a class B misdemeanor.

13 **Sec. 08.89.330. Grounds for disciplinary sanctions or denial of license.** The
14 department may impose a disciplinary sanction authorized under AS 08.89.340 on a
15 person licensed or holding a permit under this chapter or refuse to issue or renew a
16 license or permit if the department finds that the person

17 (1) used fraud or deceit in the procurement or holding of the license or
18 permit or in the application process for the license or permit;

19 (2) has been convicted of a felony in a court of competent jurisdiction,
20 either within or outside of this state, unless the conviction has been reversed and the
21 person has been discharged or acquitted, or unless the person has been pardoned with
22 full restoration of civil rights;

23 (3) is or has been afflicted with a medical problem, disability, or
24 addiction that, in the opinion of the department, impairs professional competence;

25 (4) has aided a person who is not licensed or permitted under this
26 chapter, or otherwise authorized to perform the duties of a licensee or permittee, to
27 perform diagnostic radiologic imaging, radiation therapy, or nuclear medicine
28 technology;

29 (5) has undertaken or engaged in a radiologic technology practice
30 beyond the scope of duties permitted by law;

31 (6) has, under an assumed name, impersonated a person licensed or

1 formerly licensed under this chapter or is performing duties of a fully certificated
2 licensee, a limited certificate licensee, or a person holding a permit;

3 (7) is a licensee or permittee under this chapter and has violated the
4 code of ethics established by the department;

5 (8) has interpreted a diagnostic image for a clinician, a patient, the
6 patient's family, or the public;

7 (9) is a licensee or permittee under this chapter and is or has been
8 incompetent or negligent in performance of the licensee's or permittee's duties.

9 **Sec. 08.89.340. Disciplinary sanctions.** (a) When it finds that a person
10 licensed or holding a permit under this chapter has committed an act listed in
11 AS 08.89.330, the department may impose the following sanctions singly or in
12 combination:

13 (1) permanently revoke a license to practice;

14 (2) suspend a license for a determinate period of time;

15 (3) censure a licensee;

16 (4) issue a letter of reprimand;

17 (5) place a licensee on probationary status and require the licensee to

18 (A) report regularly to the department on matters involving the
19 basis of probation;

20 (B) limit practice to those areas prescribed;

21 (C) continue professional education until a satisfactory degree
22 of skill has been attained in those areas determined by the department to need
23 improvement;

24 (6) impose limitations or conditions on the practice of a licensee.

25 (b) The department may withdraw a limitation, condition, or probationary
26 status if it finds that the deficiency that required the sanction has been remedied.

27 (c) The department may summarily suspend a license before final hearing or
28 during the appeals process if the department finds that the licensee poses a clear and
29 immediate danger to the public welfare and safety. A person is entitled to a hearing
30 conducted by the office of administrative hearings under AS 44.64.010 within seven
31 days after the suspension order is issued. A person may appeal an adverse decision

1 after hearing to the superior court.

2 (d) The department may reinstate a license that has been suspended or revoked
3 if the department finds after a hearing that the person is able to practice with
4 reasonable skill and safety.

5 Article 3. General Provisions.

6 Sec. 08.89.900. **Unified occupation for fee purposes.** For purposes of
7 AS 08.01.065, all persons licensed or holding a permit under this chapter are
8 considered to be engaged in the same occupation.

9 Sec. 08.89.910. **Regulations.** The department shall adopt regulations necessary
10 to implement this chapter.

11 Sec. 08.89.990. **Definitions.** In this chapter,

12 (1) "axial-appendicular skeleton" means the skull, including the
13 mandible, sinuses, and facial bones; spine, including cervical, thoracic, lumbar,
14 sacrum, and coccyx areas; pelvis; ribs; and upper and lower extremities;

15 (2) "contrast media" means an examination where contrast media is
16 introduced into a human body to define a part or parts not normally visualized on a
17 radiograph;

18 (3) "department" means the Department of Commerce, Community,
19 and Economic Development;

20 (4) "diagnostic radiologic imaging" means the making of film records
21 or digital records by passage of radiation through the body to act on specially
22 sensitized film or digital sensors;

23 (5) "direct supervision" means in the physical presence of a person
24 who assists, evaluates, and approves the performance of tasks;

25 (6) "knowingly" has the meaning given in AS 11.81.900(a);

26 (7) "licensed practitioner" means a physician, physician assistant,
27 nurse practitioner, podiatrist, osteopath, dentist, or chiropractor who is either licensed
28 in this state or, if practicing as a physician, podiatrist, or osteopath, is exempt from
29 licensure under AS 08.64.370(1) or (4);

30 (8) "limited radiologic imager" means a person licensed under
31 AS 08.89.150 to perform diagnostic radiologic imaging within the limits specified in

1 AS 08.89.150(b);

2 (9) "nuclear medicine technologist" means a person who prepares,
3 calibrates, and administers radiopharmaceutical agents to humans for diagnostic or
4 therapeutic purposes;

5 (10) "radiation therapist" means a person who applies radiation to
6 humans for therapeutic purposes;

7 (11) "radiographer" means a person who uses radiation on humans for
8 diagnostic purposes.

9 * Sec. 3. The uncodified law of the State of Alaska is amended by adding a new section to
10 read:

11 REGULATIONS. The Department of Commerce, Community, and Economic
12 Development may begin the process to adopt regulations to implement this Act. The
13 regulations take effect under AS 44.62 (Administrative Procedure Act) but not before the
14 effective date of the statutes implemented by the regulations.

15 * Sec. 4. Except as provided in secs. 5 and 6 of this Act, this Act takes effect July 1, 2006.

16 * Sec. 5. AS 08.89.100 and 08.89.310, enacted by sec. 2 of this Act, take effect July 1,
17 2008.

18 * Sec. 6. Section 3 of this Act takes effect immediately under AS 01.10.070(c).

FISCAL NOTE

STATE OF ALASKA
2005 LEGISLATIVE SESSION

Fiscal Note Number: 1
Bill Version: CSHB 150(L&C)
(H) Publish Date: 3/22/05

Revision Date/Time (Note if correction): _____ Dept. Affected: Commerce
Title Licensing Radiologic Technicians RDU Occupational Licensing (117)
Sponsor Anderson Component Occupational Licensing
Requester House Labor & Commerce Component No. 2360

Expenditures/Revenues (Thousands of Dollars)

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

OPERATING EXPENDITURES	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Personal Services	25.2	25.2	25.2	25.2	25.2	25.2
Travel	0.0	0.0	0.0	0.0	0.0	0.0
Contractual	6.0	6.0	6.0	6.0	6.0	6.0
Supplies	1.0	1.0	1.0	1.0	1.0	1.0
Equipment	6.0	0.0	0.0	0.0	0.0	0.0
Land & Structures						
Grants & Claims						
Miscellaneous						
TOTAL OPERATING	38.2	32.2	32.2	32.2	32.2	32.2

CAPITAL EXPENDITURES						
-----------------------------	--	--	--	--	--	--

CHANGE IN REVENUES (1156)	79.4	0.0	64.4	0.0	64.4	0.0
----------------------------------	-------------	------------	-------------	------------	-------------	------------

FUND SOURCE (Thousands of Dollars)

1002 Federal Receipts						
1003 GF Match						
1004 GF						
1005 GF/Program Receipts						
1037 GF/Mental Health						
Other 1156 - Receipt Supported Services	38.2	32.2	32.2	32.2	32.2	32.2
TOTAL	38.2	32.2	32.2	32.2	32.2	32.2

Estimate of any current year (FY2005) cost: 0.0

Check this box (X) if funding for this bill is included in the Governor's FY 2006 budget proposal:

POSITIONS

Full-time						
Part-time	1	1	1	1	1	1
Temporary						

ANALYSIS: (Attach a separate page if necessary)

HB 150 establishes licensure for occupations relating to radiologic technology. The division was advised that approximately 380 to 400 individuals will seek licensure under this bill. This fiscal note is based on the assumption there will be at least 400 licensees.

An explanation of the costs shown above are attached.

Prepared by: Jennifer Strickler, Administrative Manager Phone (907) 465-2144
Division Occupational Licensing Date/Time 2/23/05 2:02 PM
Approved by: Edgar Blatchford, Commissioner Date 2/23/2005
Agency Commerce, Community, and Economic Development

FISCAL NOTE #1

**STATE OF ALASKA
2005 LEGISLATIVE SESSION**

BILL NO. CSHB 150(L&C)

ANALYSIS CONTINUATION

HB 150: Licensing Radiologic Technicians

Total PERSONAL SERVICES: \$25.2

- Occupational Licensing Examiner I position, PPT, Range 13

This fiscal note provides funding for half of an Occupational Licensing Examiner I position to provide support to this licensing program. Last year, the division had a half time position in support of another licensing program that could have been made to full-time with this funding to support this program as well; however, that option is no longer available since that position has been assigned to support other new licensing programs. Therefore, this fiscal note identifies funding for half of a position and a corresponding position count.

Total TRAVEL: \$0

Total CONTRACTUAL SERVICES: \$6.0

- Printing, postage, communication, and advertising costs, \$3.0
- Regulations-related costs to establish education criteria and standards, and other requirements; including AAG time, \$3.0

Information has been received that licensure examinations are available from The American Registry of Radiologic Technologists. The division will seek to make arrangements with this organization for use of the licensing examinations.

Total SUPPLIES: \$1.0

To fund daily operating supplies of the program.

Total EQUIPMENT (one-time costs): \$6.0

TOTAL FISCAL NOTE: \$38.2

REVENUE: Revenue will be generated by individuals who seek license under this bill. Based on 400 licensees, each licensee can be expected to pay approximately \$176.00 biennially (\$70.4 divided by 400) in direct costs; in addition to indirect costs of approximately \$100.00 per person, for an approximate initial licensing fee of \$276.00 biennially. Licensing fees will be adjusted at the first renewal based on actual costs and numbers of licensees.



States With Licensure or Certification Laws

U.S. States with Licensure/Certification Laws or Regulations and Year of Implementation

Arizona-1977	Montana-1977
Arkansas-1999	Nebraska-1987
California-1969	New Jersey-1968
Connecticut-1993	New Mexico-1983
Delaware-1989	New York-1965
Florida-1979	North Dakota-2003
Hawaii-1974	Ohio-1995
Illinois-1990	Oregon-1979
Indiana-1982	Rhode Island-1994
Iowa-1987	South Carolina-1999
Kansas-2004	Texas-1987
Kentucky-1978	Utah-1989
Louisiana-1984	Vermont-1984
Maine-1984	Virginia-1997
Maryland-1992	Washington-1991
Massachusetts-1987	West Virginia-1977
Mississippi-1996	Wyoming-1985

States With Partial Licensure Laws and/or Other Forms of Regulation

- **Colorado** – Laws for mammography and limited (non-ARRT registered) licensure only.
- **Michigan** – Laws for mammography only.
- **Nevada** – Laws for mammography only.
- **Pennsylvania** – Technologists who have not passed the ARRT or other board-approved examination must pass a state examination to perform patient examinations in physician, osteopathic physician, podiatrist, chiropractic or dentist offices.
- **Minnesota** – Operator of any x-ray equipment for human use must be either a registered radiologic technologist through the ARRT, a licensed person from another state (and are then given an x-ray operator equivalent standing) or have passed one of Minnesota's state approved exams.
- **Tennessee** – Technologists who have not passed the ARRT or other board-approved examination must pass a state examination to perform patient examinations in physician, osteopathic physician, podiatrist, chiropractic or dentist offices.
- **Wisconsin** – Requires that all CT technologists and radiation therapists be ARRT certified.

States without Licensure Laws or With Legislative Proposals Being Considered

Alabama	Missouri
Alaska	New Hampshire
District of Columbia	North Carolina
Georgia	Oklahoma
Idaho	South Dakota



Questions and Answers About Licensure

Q *How does the unregulated practice of radiologic technology harm or endanger the public?*

A As physics and radiation biology textbooks attest, there is no threshold level for damage to healthy tissue due to ionizing radiation. In other words, there is no dose so small that it cannot potentially cause biological damage.

Q *What about alternatives to licensure such as a proficiency examination or certification by a professional association?*

A The problem with some alternatives to licensure is that they are voluntary and many health care workers will choose not to comply. State licensure programs are the most effective way to control the practice of uncredentialed individuals. As a result, licensure offers the public the best protection from unnecessary exposure to ionizing radiation and the highest quality radiologic patient care.

Q *How will the public benefit from licensure of radiologic technologists?*

A The public benefits by receiving care from properly educated and credentialed professionals who have met all of the requirements to practice radiologic technology.

Q *How do we ensure the competencies of radiologic technologists?*

A No one can be 100 percent sure of the competencies of any professional, whether in medicine, law or radiologic technology. However, steps to ensure the competence of individual practitioners can be taken. Accredited educational programs and state licensure programs are the main mechanisms for ensuring the competence of radiologic technologists. The curriculum for educational programs in radiologic technology is competency based, meaning students must meet performance objectives. The national certification examination also is a criterion-referenced, performance-based examination that has demonstrated high validity and reliability.

Q *Do the benefits of licensure justify the costs?*

A As with any endeavor, licensure requires a cost vs. benefit analysis. This is especially important in light of rising health care costs. Many states that have already implemented licensure programs saved the cost of developing an examination by contracting with the American Registry of Radiologic Technologists to use the national certification examination as their state licensing examination. Also, many states use license fees to fund their licensure program. Overall, the impact on state budgets and the health care economy are minimal.

Q *How will licensure affect the job market? Will it drive wages up, forcing employers to cut costs or raise patient fees?*

A As with any other profession or occupation, the primary objective of licensing radiologic technologists is not to create a favorable supply/demand arrangement. Rather, the objective is to restrict practice to individuals who meet certain standards and improve the quality of patient care. In California and New York, states with long-standing licensure laws, there have been no appreciable increases in average salaries for radiologic technologists since the laws passed.

Q *Won't licensure lead to fragmented care and higher health care costs, in effect creating an obstacle to health care delivery?*

A The major objective of licensure is to solve the problem of uncredentialed practitioners performing radiologic examinations on human beings. Related objectives are to reduce unnecessary radiation exposure and reduce costs associated with repeat examinations. Far from creating obstacles, properly educated and credentialed practitioners streamline health care and ensure the highest possible quality of care.



American Society of
Radiologic Technologists

March 4, 2005

The Honorable Tom Anderson
Alaska House of Representatives
State Capitol Building, Room 408
Juneau, AK 99801-1182

Dear Representative Anderson:

The American Society of Radiologic Technologists, representing more than 116,000 medical imaging professionals nationally including 350 in Alaska, is pleased to hear of your introduction of HB 150 before the Alaska Legislature.

The ASRT's goals are educating the medical community and the public about the benefits and risks of radiologic and other diagnostic medical procedures while providing safe, effective examinations and treatments to patients. ASRT firmly believes that personnel performing diagnostic and therapeutic procedures on patients must be required to demonstrate competence through education and certification.

ASRT has pursued these goals by supporting the federal Consumer-Patient Radiation Health and Safety Act of 1981, which established basic certification and education guidelines for personnel who perform radiologic procedures. However there was no enforcement provision in this act, leaving the adoption of certification and education standards to the discretion of each state. To date, 41 states have enacted licensure, certification laws or regulations for medical imaging and radiation therapy professionals and the regulations vary widely from state to state. Hopefully Alaska will be the 42nd state to enact a law that guarantees that all members of the public—young, old, male and female—receive safe and high-quality radiologic examinations and treatments.

We have worked closely with our state affiliate society, the Alaska Society of Radiologic Technologists, to advocate education and credentialing standards for persons who perform medical imaging, plan and deliver radiation therapy treatments for Alaska's citizens. Please feel free to call upon me in the ASRT Government Relations department if I can be of further assistance.

Sincerely,

A handwritten signature in black ink that reads "David R. Harwell". The signature is written in a cursive style with a large, sweeping initial "D".

David R. Harwell
State Legislative Coordinator