The Florida Senate

PROFESSIONAL STAFF ANALYSIS AND ECONOMIC IMPACT STATEMENT

(This document is based on the provisions contained in the legislation as of the latest date listed below.)

Prepared By: Commerce Committee

BILL:	CS/SB 694
INTRODUCER:	Commerce Committee and Senator Aronberg
SUBJECT:	Caller ID Anti-spoofing Act
DATE:	March 5, 2008 REVISED:

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Rogers	Cooper	CM	**Fav/CS**
2.			CJ	
3.			JU	
4.				
5.				
6.				

Please see Section VIII. for Additional Information:

A. COMMITTEE SUBSTITUTE.....	X	Statement of Substantial Changes
B. AMENDMENTS.....		Technical amendments were recommended
		Amendments were recommended
		Significant amendments were recommended

I. Summary:

This CS prohibits entering or causing to be entered false information into a telephone caller identification system with the intent to deceive, defraud, or mislead. It also prohibits placing a call knowing that aforementioned information was entered into the telephone caller identification system.

It provides exceptions for federal, state, county or municipal government law enforcement agencies, any Federal intelligence or security agency, and telecommunications, broadband, or VoIP service providers that are acting solely as intermediaries for the transmission calls.

It provides for the enhancement of penalties when a violation is committed during or facilitates the commission of a criminal offense, and that a violation is an unlawful trade practice under specified provisions.

This CS creates section 817.487 of the Florida Statutes.

II. Present Situation:

Caller Identification or "Caller ID" allows an individual to identify a caller before answering the telephone. It is an optional telephone service, although it is now a standard feature on many cellular phones, traditional telephone services, and Voice over Internet Protocol (VoIP) services. A caller's number or name is displayed either on the phone or an external display unit. The number or name will appear on the display unit or on the phone after the first ring.

Caller ID can be manipulated and used for fraudulent purposes. Using a practice known as "caller ID spoofing," individuals, groups, or corporations change the telephone number that is displayed on the caller ID in an effort to withhold or disguise the identity or originator of the call.[1]

Technology

Signaling System 7 (SS7) enables caller ID to function. The public switched telephone network (PSTN) is the network on which traditional phone calls are placed. The PSTN is a worldwide network. SS7 routes the calls that are placed on the PSTN. SS7 allows the call originator's local telephone exchange to send a Calling Party Number (CPN), which includes the number of the caller and whether or not the caller wants their number to be blocked.[2] When a telecommunications carrier uses SS7 to set up a call, the Federal Communications Commission (FCC) regulations require that the CPN must be transmitted. Also per FCC regulation, consumers can dial *67 to conceal their CPN.[3]

Caller ID spoofing is accomplished by manipulating the SS7 information associated with the call.[4] The automatic number identification (ANI) is a service that transmits the billing telephone number along with the telephone number of the incoming call.[5] While the CPN can be manipulated, the ANI cannot be. Most emergency lines (911) are set up to receive both the CPN and the ANI, making it more difficult for a caller to withhold or change information.[6] At the time of this analysis, the Florida Department of Law Enforcement Computer Crimes Center stated that the department does not have the technology in place to uncover the ANI associated with a call in the course of an investigation.[7]

Caller ID technology has grown more complex due to the increased popularity of VoIP services. An internet application utilized by VoIP involves "packet-switching."[8] Packet-switching uses a broadband internet connection to transmit voice communication. At the time of this analysis, FCC regulations do not apply to VoIP service providers in the same manner that they apply to

---

[1] Federal Communications Commission (FCC), "Caller ID and Spoofing, FCC Consumer Facts", November 30, 2007, http://www.fcc.gov/cgb/consumerfacts/callerid.html.
[2] Florida Department of Law Enforcement Computer Crimes Center, conversation with staff. January 18, 2008.
[3] Memorandum addressed to the United States Senate Commerce Committee, June 19, 2007.
[4] Written Statement on Caller ID Spoofing, to the Committee on Commerce, Science, and Transportation, United States Senate, by Kris Anne Monteith, Chief, Enforcement Bureau, Federal Communications Commission. June 21, 2007, http://www.fcc.gov/eb/speeches/kris070621.pdf.
[5] See http://www.pcmag.com/encyclopedia_term/0,2542,t=automatic+number+identification&i=37775,00.asp.
[6] See http://www.calleridspoofing.info/frequently-asked-questions.php.
[7] Florida Department of Law Enforcement Computer Crimes Center, conversation with staff. January 18, 2008.
[8] See http://en.wikipedia.org/wiki/Packet_switching.

traditional telephone service. A consumer or business utilizing VoIP services are able to use web settings to control the features of their phone service. This control extends far beyond that available to an individual using a traditional telephone system.[9] The caller ID information that is distributed when a call is made can be changed by customers subscribing to certain VoIP services.[10]

With the advent of VoIP, it has become simpler for callers to transmit misleading CPN information. This is a contrast to several years ago when a special phone connection and expensive equipment were required to engage in spoofing.[11] There are numerous websites that will allow callers to remain anonymous through the use of spoofing technology. These sites require the user to register and provide certain personal information. These sites charge a nominal fee (as little as $10 for 60 minutes of call time).[12] One of these sites also sells its calling card services in retail stores throughout the United States, and both these cards and the website were recently featured in a major motion picture.[13] A caller utilizing one of these services has the ability to call a toll-free number, enter a name or any destination number (such as a number that belongs to another individual, business, or government entity) of their choosing and the Caller ID of the individual who is receiving the call will display the name or telephone number that was selected, instead of displaying the actual number the call is originating from. Additional features available include the ability to change the caller's voice to male or female, and the ability to record the conversation for later retrieval.[14]

Additionally, the program that these websites use is easy to locate online and can be downloaded by an individual who has knowledge of the technology and can be then operated from an individual computer.

Uses

There are various known uses for spoofing technologies. These include:

- Businesses and corporations use spoofing to display an individuals work telephone number while they are calling from another phone, such as a cell phone;[15]
- Federal, state and local law enforcement uses spoofing for various investigative purposes;
- Bounty Hunters and Private Investigators use spoofing to track individuals;
- Domestic Violence Shelters use spoofing technology to prevent the disclosure of the shelter location;[16]
- Voicemail hacking;

[9] See http://en.wikipedia.org/wiki/Voice_over_IP.
[10] Florida Department of Agriculture and Consumer Services, Division of Consumer Services, Florida Consumer E-Newsletter, May 2006 http://www.800helpfla.com/newsletter/2006/052006.html.
[11] See http://en.wikipedia.org/wiki/Voice_over_IP.
[12] See www.spoofcard.com, www.telespoof.com, www.phonegangster.com, http://teltechcorp.com.
[13] See http://www.officialspoofcard.com/spoofcard-untraceable-movie.php.
[14] See http://www.spoofcard.com/faq.php#q3.
[15] Testimony and Statement before Committee on Commerce, Science, and Transportation, United States Senate, from Allison Knight, Staff Counsel, Electronic Privacy Information Center (EPIC), June 21, 2007 http://commerce.senate.gov/public/index.cfm?FuseAction=Hearings.Testimony&Hearing_ID=1878&Witness_ID=6655.
[16] See *Id.*

- "Swatting," which is making a false report of an emergency to a police department for the purpose of causing a Special Weapons and Tactics (SWAT) response to a physical address;[17]
- Wire transfer fraud;[18]
- "Phone Phishing, which is an attempt to criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication;"[19]
- Bomb Threats; and
- Prank calls.

The Florida Department of Financial Services, Division of Insurance Fraud, circulated a bulletin to local law enforcement in July of 2007. This bulletin lists possible uses for spoofing technology and the threat posed to Florida citizens using this technology.[20]

Florida Caller ID Law for Telephone Solicitors

Section 501.059(7), F.S., addresses telephonic sales calls and the requirements for caller identification during such calls, which would preclude spoofing.[21] This provision makes it unlawful for

> "any person who makes a telephonic sales call or causes a telephonic sales call to be made to fail to transmit or cause not to be transmitted the telephone number and, when made available by the telephone solicitor's carrier, the name of the telephone solicitor to any caller identification service in use by a recipient of a telephonic sales call."

In addition, it is unlawful for such callers to

> "intentionally alter the voice of the caller in an attempt to disguise or conceal the identity of the caller in order to defraud, confuse, or financially or otherwise injure the recipient of a telephonic sales call or in order to obtain personal information from the recipient of a telephonic sales call which may be used in a fraudulent or unlawful manner."

---

[17] In United States of America v. Stuart Rosoff, No. 3:07-CR-0196-B, Filed November 2, 2007, in the US District Court for the Northern District of Texas, Dallas Division, Mr. Rosoff pled guilty to various crimes, including "swatting"; which resulted in the injury of at least two victims; one individual was an elderly man residing in New Port Richey, Florida.
[18] Memorandum addressed to the United States Senate Commerce Committee, June 19, 2007.
[19] See http://en.wikipedia.org/wiki/Phishing, Jefferson City News Tribune, Online Edition. "Warning! Scam to steal personal information shows bank on caller ID" March 1, 2007;
http://www.newstribune.com/articles/2007/03/01/news_local/305local02cbscam.prt
AARP Alerts, "Colorado Springs Police Protective Association Name is Being Spoofed to Get Donations" April 2, 2007, http://www.aarpelderwatch.org/public/alerts/cs_prot_scam.html;
The Columbus Dispatch, Online Edition. "Callers Pose as Police Using Phone Spoof." December 7, 2007, http://www.dispatch.com/live/content/local_news/stories/2007/12/07/phonespoof.html.
[20] Department of Financial Services, Division of Insurance Fraud, Intelligence Bulletin, July 20, 2007.
[21] Telemarketers are regulated by the Department of Agriculture and Consumer Services in the Florida Telemarketing Act, ss. 501.601-626, F.S. These provisions require telemarketers, within the first 30 seconds of a telephone call, to identify themselves by stating their name, the company on whose behalf the solicitation is being made, and the consumer goods or services being sold. *See* s. 501.613(1), F.S.

Violators of this statute are subject to civil penalties or injunctive relief, in an amount not to exceed $10,000 per violation. To date, no penalties or injunctions have been filed in instances where the caller used a spoofing mechanism.[22]

Federal Communications Commission Action

The Federal Communications Commission's (FCC) efforts to address ID spoofing began in 1995. Pursuant to the Telephone Consumer Protection Act, the FCC adopted rules that require all telecommunications carriers using SS7 to transmit the CPN associated with an interstate call to interconnecting carriers.[23] Federal Communications Commission (FCC) rules prohibit telemarketers from blocking Caller ID information and require them to provide accurate caller ID numbers.[24] FCC rules require that a telemarketer:

- "transmit or display its telephone number, and, if possible, its name or the name and telephone number of the company for which it is selling products or services,
- display a telephone number that can be called during regular business hours to ask to no longer be called. This rule applies even to companies that already have an established business relationship with a consumer.

For violations of these rules, the FCC can seek a monetary fine. If the violator is not an FCC licensee, the FCC must first issue a warning and the telemarketer may be fined only for violations committed after the warning."[25]

The Enforcement Bureau of the FCC has initiated investigations of thirteen companies that sell caller ID spoofing services. One investigation resulted in a citation against a telemarketer.[26] FCC rules governing the duty to transmit CPN apply to common carriers, or providers of telecommunications service. As VoIP has not yet been classified as either a "telecommunications service" or "information service," the application of these rules to VoIP providers has not been established. The agency's enforcement options may be limited because many of the web-based entities offering ID spoofing services are not service providers directly regulated by the FCC,[27] and several of these web based entities are not located within the United States.

Pending Legislation[28]

H.R. 251, the Truth in Caller ID Act of 2007, was introduced in the United States House of Representative's in January 2007. H.R. 251 amends the Communications Act to make it

[22] Statement given by the Florida Department of Agriculture and Consumer Services staff, January 15, 2008.
[23] Memorandum addressed to the United States Senate Commerce Committee, June 19, 2007.
[24] See http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=1487980001.
[25] Federal Communications Commission (FCC), "Caller ID and Spoofing, FCC Consumer Facts", November 30, 2007, http://www.fcc.gov/cgb/consumerfacts/callerid.html.
[26] Written Statement on Caller ID Spoofing, to the Committee on Commerce, Science, and Transportation, United States Senate, by Kris Anne Monteith, Chief, Enforcement Bureau, Federal Communications Commission. June 21, 2007, http://www.fcc.gov/eb/speeches/kris070621.pdf.
[27] Memorandum addressed to the United States Senate Commerce Committee, June 19, 2007.
[28] *Id.*

unlawful "to transmit misleading or inaccurate caller identification information, with the intent to defraud or cause harm." Exemptions are provided for law enforcement and intelligence agencies. The bill was reported by the Energy and Commerce Committee on June 11, 2007, and passed by the House on June 12, 2007, and has been referred to the U.S. Senate Commerce Committee.

In the United States Senate, S. 704, the Truth in Caller ID Act of 2007, was introduced in February 2007. If enacted, the bill would amend the Communications Act of 1934 to make it unlawful "to transmit misleading or inaccurate caller identification information." This bill provides a law enforcement exemption. On December 5, 2007, the Committee on Commerce, Science, and Transportation amended the bill and it was then placed on Senate Legislative Calendar.

H.R. 740, the Preventing Harassment through Outbound Number Enforcement (PHONE) Act of 2007, was reported by the House Judiciary Committee on March 8, 2007, and passed by the House on March 21, 2007. H.R. 740 would make it unlawful to use or provide "false caller ID information with intent to defraud; . . . or caller ID information pertaining to an actual person without that person's consent and with intent to deceive the recipient of a call about the identity of the caller." Violations are punishable by imprisonment of up to 5 years. It also has a law enforcement exception. The U.S. Senate Judiciary Committee reported H.R. 740, with amendments, on May 24, 2007.

III. Effect of Proposed Changes:

Section 1 provides that the act should be cited as the "Caller ID Anti-Spoofing Act."

Section 2 creates s. 817.487, F.S., to prohibit what has been described as "Caller ID spoofing" (or "phone spoofing" or "spoofing"). The prohibited conduct constituting "Caller ID spoofing" consists of the following: (1) entering or causing to be entered false information into a telephone caller identification system with the intent to deceive, defraud, or mislead the recipient of a call or the network itself; or (2) placing a call knowing that false information was entered into the telephone caller identification system with the intent to deceive, defraud, or mislead the recipient of the call or the network itself. The CS defines key terms relevant to the prohibited acts:

- Call means any type of telephone call made using a public switched telephone network, wireless cellular telephone service, or voice-over-Internet protocol (VoIP) service that has the capability of accessing users on the public switched telephone network or a successor network. Caller means a person who places a call, whether by telephone, over a telephone line, or on a computer.
- Enter means to input data by whatever means into a computer or telephone system.
- False information means data that misrepresents the identity of the caller to the recipient of a call or to the network itself; however, when a person making an authorized call on behalf of another person inserts the name, telephone number, or name and telephone number of the person on whose behalf the call is being made, such information shall not be deemed false information.

- Telephone caller identification system means a listing of a caller's name, telephone number, or name and telephone number that is shown to a recipient of a call when it is received.

The CS provides exceptions to application of the new section:

- The blocking of caller identification information.
- Any law enforcement agency of the federal, state, county, or municipal government.
- Any intelligence or security agency of the Federal Government.
- Telecommunications, broadband, or VoIP service providers that are acting solely as intermediaries for the transmission calls.

The CS provides that the prohibited acts are first degree misdemeanors.[29] The CS also provides that these prohibited acts constitute an unlawful trade practice under the Florida Deceptive and Unfair Trade Practices Act,[30] and, in addition to any remedies or penalties set forth in the section, are subject to any remedies or penalties available for a violation of that part.

The CS also provides that the felony or misdemeanor degree of any criminal offense shall be reclassified by the court to the next higher degree if the offender committed either of the prohibited "Caller ID spoofing" acts during the commission of the criminal offense or if the court finds that the prohibited "Caller ID spoofing" acts facilitated or furthered the criminal offense. The reclassification shall be as follows:

- In the case of a second degree misdemeanor,[31] the offense is reclassified as a first degree misdemeanor.
- In the case of a first degree misdemeanor, the offense is reclassified as a third degree felony.[32]
- In the case of a third degree felony, the offense is reclassified as a second degree felony.[33]
- In the case of a second degree felony, the offense is reclassified as a first degree felony.[34]
- In the case of a first degree felony punishable by a term of imprisonment not exceeding life, the offense is reclassified as a life felony.[35]

For purposes of sentencing under ch. 921, F.S., (the Criminal Punishment Code),[36] the following offense severity ranking levels apply:

[29] Pursuant to ss. 775.082 and 775.083, F.S., a first degree misdemeanor is punishable by up to 1 year imprisonment in jail and a $1,000 fine.
[30] Part II of ch. 501, F.S.
[31] Pursuant to ss. 775.082 and 775.083, F.S., a second degree misdemeanor is punishable by up to 60 days in jail and a $500 fine.
[32] Pursuant to ss. 775.082 and 775.083, F.S., a third degree felony is punishable by up to 5 years in state prison and a $5,000 fine.
[33] Pursuant to ss. 775.082 and 775.083, F.S., a second degree felony is punishable by up to 15 years in state prison and a $10,000 fine.
[34] Pursuant to ss. 775.082 and 775.083, F.S., a first degree felony is generally punishable by up to 30 years in state prison and a $10,000 fine.
[35] Pursuant to ss. 775.082 and 775.083, F.S., a life felony is generally punishable by a term of imprisonment for life or by imprisonment for a term of years not exceeding life imprisonment and a $15,000 fine.

- An offense that is a first degree misdemeanor and that is reclassified as third degree felony is ranked in level 2 of the offense severity ranking chart.
- A felony offense that is reclassified is ranked one level above the ranking specified in s. 921.0022, F.S., or s. 921.0023, F.S., for the offense committed.

Provided is an illustration of how the reclassification might be applied. If a person committed a first degree misdemeanor by obtaining a credit card by fraudulently using personal information of another person, the first degree misdemeanor would be reclassified to a third degree felony if this person obtained the credit card by calling the issuer of the card and the call involved "Caller ID spoofing." The third degree felony would be ranked in Level 2 for purposes of determining the scored lowest permissible sentence under the Criminal Punishment Code. Further, the maximum penalty would substantially increase because of the reclassification, since the maximum penalty for a first degree misdemeanor is 1 year in a jail and the maximum penalty for a third degree felony is 5 years in state prison.

Section 3 provides an effective date of October 1, 2008.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

None.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

V. Economic Impact and Fiscal Note:

A. Tax/Fee Issues:

None.

[36] The Criminal Punishment Code ("code"), Florida's general sentencing law, applies to all felonies, except capital felonies. Felony offenses are either ranked in the code's offense severity level ranking chart, s. 921.0022, F.S., or if not ranked in the chart, are ranked pursuant to s. 921.0023, F.S., based on their felony degree. Sentencing points are assessed based on the ranking of the primary offense, additional offenses, and other factors, which are entered into a calculation to determine the lowest permissible sentence. Absent mitigation (reduction) of sentence based on permissible mitigating factors, the sentencing range is the lowest permissible sentence up to, and including, the maximum penalty for the felony degree of the offense. In order for a first-time offender who has committed only a single felony to score a lowest permissible sentence of state prison, the felony must be ranked in level 7 or above (there are 10 levels with level 10 being the most serious level).

B. Private Sector Impact:

None.

C. Government Sector Impact:

The CS provides for felony and misdemeanor reclassifications, and therefore is subject to review by the Criminal Justice Impact Conference (CJIC). CJIC estimates that the CS has an indeterminate (unquantifiable) prison bed impact.

VI. Technical Deficiencies:

None.

VII. Related Issues:

None.

VIII. Additional Information:

A. Committee Substitute – Statement of Substantial Changes:
(Summarizing differences between the Committee Substitute and the prior version of the bill.)

This Committee Substitute:

- Clarifies the definitions of "call" and "false information."
- Specifies that a person may not "cause to be entered" false information into a telephone identification system.
- Provides an exemption from liability for a telecommunications, broadband, or VoIP service provider that is acting solely as an intermediary for the transmission of the call.
- Reorders the penalty subsection so that it now precedes the reclassification subsection.
- Deletes a provision that implied judges would decide whether this law was violated during the commission of a crime.
- Deletes an archaic reference to gain-time eligibility.

B. Amendments:

None.