SENATE COMMITTEE ON ENERGY, UTILITIES AND COMMUNICATIONS
Senator Ben Hueso, Chair
2019 - 2020 Regular

Bill No:	AB 1132	**Hearing Date:**	6/18/2019
Author:	Gabriel		
Version:	5/16/2019 As Amended		
Urgency:	No	**Fiscal:**	Yes
Consultant:	Sarah Smith		

SUBJECT: Telecommunications: caller identification fraud

DIGEST: This bill prohibits the falsification of a state or local agency's caller identification (caller ID) information with the intent to mislead, cause harm, deceive, or defraud the recipient of the call.

ANALYSIS:

Existing law:

1) Authorizes the California Public Utilities Commission (CPUC) to regulate the use of autodialing devices within the state and establishes specified restrictions on the use of those devices. (Public Utilities Code §2871 et. seq.)

2) Establishes telecommunications customer right of privacy protections prohibiting the disclosure of a residential subscriber's personal information without obtaining consent for the disclosure in writing. The right to privacy prohibits the disclosure of information that includes, but is not limited to the following:
   a) Personal calling patterns
   b) Credit and financial information
   c) Information identifying services purchased by the subscriber
   d) Specific or aggregated demographic information that includes individual identities and characteristics. (Public Utilities Code §2891)

3) Prohibits telephone corporations from disclosing subscribers' unpublished or unlisted telephone numbers on residential subscriber lists that the corporations sells or licenses. A subscriber may waive this protection by providing the telephone corporation with a written notice. (Public Utilities Code §2891.1(a))

4) Prohibits wireless telecommunications providers and their affiliates from disclosing the name and telephone number of a subscriber unless the subscriber

expressly provides consent for the disclosure. (Public Utilities Code §2891.1(b))

5) Allows a subscriber to revoke a prior authorization to disclose subscriber information at any time. Wireless telecommunications providers must comply with a revocation within 60 days. (Public Utilities Code §2891.1(d))

6) Requires the CPUC to direct each wireless telecommunications provider to report on activities related to customer fraud. These reports must include the types of fraud, the amount of resulting uncollected revenues, and the actions taken by the wireless provider to combat fraud. The CPUC must require wireless provider to supply their subscribers with a notice, reviewed by the CPUC, warning consumers about the dangers of fraud and methods for protecting themselves against fraud. (Public Utilities Code §2892.3)

7) Requires the CPUC to direct each telephone caller ID service to allow a caller to withhold the caller's telephone number from display on an individual basis. Callers cannot withhold the display of business phone numbers used for telemarking purposes. (Public Utilities Code §2893)

8) Prohibits the use of telecommunications systems for the creation of false caller ID numbers with the intent to defraud, cause harm, or wrongfully obtain anything of value, and establishes penalties for violations. The attorney general of a state may bring a civil action on behalf of residents in federal court to enforce federal prohibitions against illegal uses of caller IDs or impose civil penalties for violations whenever the officer has reason to believe that the interests of the state's residents have been or are being threatened or adversely affected. States are not preempted from adopting intrastate statutes that are more restrictive than federal law on the use of telecommunications equipment for certain purposes, including telephone solicitations, auto-dialers, pre-recorded or artificial messages, and unsolicited fax advertisements. (Title 47 United States Code §227(e-f))

9) Authorizes the attorney general of a state, or an official or agency designated by a state, has reason to believe that any person has engaged or is engaging in a pattern or practice of telephone calls or other transmissions to residents of that state in violation of this section or the regulations prescribed under this section, the state may bring a civil action on behalf of its residents to enjoin such calls and/or pursue civil penalties for each violation. (Title 47 United States Code §227 (g))

This bill:

1) Prohibits the falsification of a state or local agency's caller ID information with the intent to mislead, cause harm, deceive, or defraud the recipient of the call.

2) Exempts the following from the prohibition on government agency caller ID spoofing:
   a) Blocking of caller ID information
   b) Law enforcement agencies
   c) Federal intelligence or security agencies
   d) Telecommunications providers acting solely as an intermediary for the transmission of telecommunications service between the caller and the recipient.

3) Specifies that violators of the government agency prohibition are subject to the following actions:
   a) Enjoinment in any court with jurisdiction
   b) A civil penalty of up to $10,000 for each violation

4) Allows city attorneys, district attorneys, and the attorney general to enforce the bill.

5) Requires the CPUC to notify the attorney general and appropriate district attorney if it discovers that a spoofing violation has occurred when investigating the use of autodialing devices in the state.

Background

What is spoofing, and why is it so harmful? In telecommunications, spoofing occurs when a caller conceals his or her identity by using a fake caller ID. Generally, spoofed calls are placed through a computer using a Voice Over Internet Protocol (VoIP) phone system, which transmits calls over an internet-based network and into traditional telephone and wireless telephone systems. When using these VoIP systems, spoofers can use a computer application for autodialing that allows them to create a fake caller ID that is displayed on the recipient's phone.

Spoofed caller ID can be used for lawful purposes. For example, doctors' offices can create a spoofed caller ID when sending robocalls to remind patients of upcoming appointments. These spoofed IDs are intended to prevent the patient from reverse dialing the appointment reminder system. When legitimate businesses conduct spoofed calls, they obtain approval to use these caller IDs and

must comply with specific rules, including Federal Communications Commission (FCC) "do not call" requirements.

Some scammers pick a specific phone number to spoof as part of a scam, including phone numbers for government offices. For example, spoofers have hijacked the phone numbers of the Internal Revenue Service, Social Security Administration, local electrical and gas utilities, and law enforcement offices. According to the Federal Trade Commission (FTC), government imposter scams generated approximately 50 percent of the imposter scam reports submitted to the FTC in 2018. A 2018 spoofing scam in which scammers hijacked the phone number of Social Security Administration in an attempt to steal social security numbers generated a significant number of these complaints. Spoofing a government agency phone number can be particularly harmful to low-income consumers and vulnerable populations who may have more regular contact with and reliance upon government programs and their offices.

Spoof busting: who you gonna call? Existing federal law prohibits caller ID spoofing with the intent to defraud, cause harm, or wrongfully obtain anything of value, and establishes penalties for violations. This bill establishes a specific state-level prohibition on spoofing state and local government caller IDs and establishes state-level penalties in addition to those that exist at the state level. Despite the presence of prohibitions and penalties, spoofing calls continue to grow and elude enforcement actions. Since spoofers hijack and fake caller IDs to conceal their identity and circumvent call-blocking technology, tracking the calls, identifying violators, and taking enforcement action has been challenging. Without a mechanism to identify the real location from which scam calls are placed, the CPUC and law enforcement officials will still face obstacles to enforcing the prohibitions and penalties contained in this bill.

Dual referral. Should this committee approve this bill, it will be re-referred to the Senate Committee on Judiciary for their consideration.

Prior/Related Legislation

SB 208 (Hueso, 2019) would require telecommunications providers to implement a caller ID authentication system by July 1, 2020. The bill also authorizes the CPUC to work with the attorney general to enforce federal prohibitions against illegal caller ID spoofing. The bill is pending consideration in the Assembly Committee on Communications and Conveyance.

FISCAL EFFECT: Appropriation: No Fiscal Com.: Yes Local: No

SUPPORT:

Consumer Federation of California (Sponsor)
The Utility Reform Network

OPPOSITION:

None received

ARGUMENTS IN SUPPORT: According to the author:

> While there are legitimate reasons for spoofing certain types of calls, a call identifying itself as coming from a government entity is inherently misleading. The practice has been used to imbue the call with the appearance of authority, increase the likelihood someone answers the call, and defraud unsuspecting consumers.
>
> AB 1132 will prohibit any person from impersonating, "spoofing", the caller ID information of a federal, state, or local governmental entity. This bill will also prohibit placing a call knowing this information has been falsely impersonated.

-- END --