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

Bill No:	SB 208	**Hearing Date:**	3/27/2019
Author:	Hueso		
Version:	2/4/2019 As Introduced		
Urgency:	No	**Fiscal:**	Yes
Consultant:	Sarah Smith		

SUBJECT: Consumer Call Protection Act of 2019

DIGEST: This bill requires telecommunications providers to implement caller identification (caller ID) authentication protections by July 1, 2020. It also allows the California Public Utilities Commission (CPUC) to coordinate with the Attorney General to enforce federal prohibitions on illegal robocalls in California.

ANALYSIS:

Existing law:

1) Prohibits unjust or unreasonable charges, practices, classifications, and regulations for or regarding common carrier interstate communications services by wire or radio. The Federal Communications Commission (FCC) is authorized to establish rules and regulations to enforce these requirements. (47 United States Code §202)

2) Defines interconnected Voice Over Internet Protocol (VOiP) as a service that enables real-time, two-way voice communications, requires a broadband connection from the user's location, requires internet compatible equipment and permits users to receive and terminate calls via the public switched telephone network. VOiP is also classified as an "Advanced Communications Service. (Title 47 United States Code §153 and Title 47 Code of Federal Regulations §9.3)

3) Requires the FCC and state agencies with telecommunications regulatory authority to encourage the deployment of advanced telecommunications capability to all Americans in a reasonable and timely manner. These agencies must exercise this authority in a manner consistent with the public interest, convenience, necessity, price cap regulation, regulatory forbearance, methods for encouraging local telecommunications market competition, or other regulatory methods for removing barriers to infrastructure investment. Advanced telecommunications capability is defined as high-speed, switched,

broadband telecommunications capability that enables users to originate and receive high-quality voice, data, graphics, and video telecommunications using any technology. (47 United States Code §1302/ Telecommunications Act of 1996 §706)

4) Authorizes the CPUC to fix rates, establish rules, examine records, issue subpoenas, administer oaths, take testimony, punish for contempt, and prescribe a uniform system of accounts for all public utilities subject to its jurisdiction. (California Constitution, Article XII, §6)

5) Defines the term "public utility" and includes common carriers in the definition of a public utility. (Public Utilities Code §216)

6) Gives the CPUC the authority to supervise and regulate every public utility in the state and do all things necessary and convenient in the exercise of such power and jurisdiction. (Public Utilities Code §701)

7) States California's telecommunications policy, including affirming the State's commitment to universal service by assuring the continued affordability and widespread availability of high-quality telecommunications services to all Californians; encouraging expanded access to state-of-the-art technologies for rural, inner-city, low-income, and disabled Californians; promoting lower prices, broader consumer choice, and avoidance of anticompetitive conduct; and encouraging fair treatment of consumers through the provision of sufficient information for making informed choices, establishment of reasonable service quality standards, and establishment of processes for equitable resolution of billing and service problems. (Public Utilities Code §709)

8) Prohibits the CPUC and any department, agency, commission, or political subdivision of the state from exercising regulatory authority over VOiP and internet protocol (IP) enabled services unless required or expressly delegated by state or federal law. Any delegation or express requirement does not expand the jurisdiction of the CPUC, department, agency, or subdivision beyond the scope of that requirement or delegation. (Public Utilities Code §710)

9) Prohibits the use of telecommunications systems for the creation of false caller ID numbers with the tent 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))

10) 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) Requires each telecommunication provider within the state to implement Secure Telephony Identity Revisited and Secure Handling of Asserted information using toKENs (STIR/SHAKEN) or a similar caller ID authentication system by July 1, 2020.

2) Designates the Attorney General and CPUC as the appropriate state agencies for implementing the Truth in Caller ID Act within California and authorizes these agencies to exercise authority granted to states under the Truth in Caller ID Act.

3) Expressly authorizes the CPUC to work with the Attorney General to enforce the Truth in Caller ID Act within California.

Background

The robocall epidemic and its impact on telecommunications. Telecommunications providers are not the source of illegal robocalls, but their platforms are the delivery method. Robocalls are the top consumer complaint to the FCC; in 2018, the FCC received 232,000 complaints from consumers regarding robocalls. According to data from call blocking companies that monitor robocalls, Americans received approximately five billion robocalls between January and February of 2019. Of all states, California receives the second highest number of robocalls in the nation (Texas receives the most robocalls of any state). Los Angeles, San Francisco, San Diego, and Riverside are listed in the top 20 cities receiving the highest volume of robocalls. While certain robocalls are legitimate attempts to contact consumers, an increasing number of calls are fraudulent. Experts estimate that by 2020, 40

percent of all calls received in the United States will be fraudulent calls. According to the Federal Trade Commission (FTC), fraud generates the greatest number of complaints to the FTC. In 2018, the FTC received over 1.4 million complaints regarding fraud, and approximately 70 percent of those frauds started over the telephone.

The high volume of illegal robocalls has negatively impacted all consumers' ability to use telecommunications services as consumers are advised to simply not answer their phone to prevent exposure to fraud. However, robocall scams disproportionately impact more vulnerable populations. According to FTC, when consumers over the age of 70 lost money to a scam, their losses were significantly larger than younger victims. Some robocall scams have targeted specific populations, including military service families and non-English speaking populations. The degree to which individuals perpetuating these scams are using telecommunications technology to conceal their identity and pose as trustworthy institutions also makes combatting the calls challenging.

Spoofing, especially neighbor spoofing, is driving robocall scams. Call 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 VOiP phone network. VOiP systems turn voice calls into data that can be transmitted over internet-based networks and into traditional and wireless telephone 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.

Some entities use a spoofed caller ID for beneficial purposes. For example, doctors' offices may spoof a caller ID when sending robocalls to remind patients of upcoming appointments. These spoofed calls are intended to prevent the patient from reverse dialing the appointment reminder system. When legitimate businesses conduct spoofed calls, they generally rent or obtain approval to use the caller IDs from which they are calling. These callers comply with specific rules, including FCC "do not call" requirements.

Neighbor spoofing is a type of caller ID spoofing in which a robocaller hijacks a local phone number to pose as a local caller. The spoofer calls consumers within that area code, tricking consumers into answering a call they believe is local. Consumers frequently answer these calls expecting to speak with a local business, government office, family member, or friend. Instead, they usually receive a pre-recorded message attempting to scam the consumer out of money or personal information.

The FTC has acknowledged that neighbor spoofing is key to conducting scams over the telephone because it increases the frequency with which people answer scam calls. Consumers also cannot effectively use self-reported call blocking services because the spoofed caller ID conceals the real source of the call. Frequently, neighbor spoofers will pick a geographic region to target, generate a local number as a caller ID, and use a computer-based autodialing system to call thousands of people within the targeted region. Some spoofers pick a specific phone number to use as part of a scam. 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.

What is STIR/SHAKEN and how does it work? This bill requires telecommunications providers to implement STIR/SHAKEN or similar form of caller ID authentication system. STIR/SHAKEN is a set of caller ID authentication protocols that use computer programming to determine if a caller ID has been spoofed. The programming is embedded into telecommunication network controls, and uses data about the call to determine the degree to which the call is likely spoofed. The system attaches a digital signature based on the ability to verify the source and veracity of the caller ID, and that signature is transmitted with the phone call across telecommunications networks. The final network transmitting the call to the consumer will use a digital key to verify that the signature is correct. If the signature is verified, the caller ID should match the source of the call.

Authentication is not a silver bullet, but it is an important first step. Caller ID authentication by itself does not stop calls; however, it is a tool that telecommunications providers and consumers can use to identify spoofed calls and fully verified calls. Identifying spoofed calls is the first step to filtering illegal robocalls and reducing the likelihood of successful scams. Identifying these illegal robocalls is also an important component of enforcing consumer protections that already exist.

Existing law already prohibits illegal robocalls and establishes penalties. However, caller ID spoofing limits the degree to which law enforcement can identify the source of calls for investigation and prosecution. To the extent that illegal robocalling operations exist within California, the lack of caller ID authentication may be preventing California from enforcing consumer protections. This bill designates the CPUC as an appropriate agency to work with the Attorney General to support action against individuals and entities that violate the Federal Truth in Caller ID Act, which prohibits illegal robocalls and specifies penalties. The CPUC is the only state agency with experience monitoring telecommunications service quality issues

This bill supports efforts at the federal level. Federal law prohibits spoofing with the intent to defraud, cause harm, or wrongfully obtain anything of value. Telecommunications providers are updating the FCC on efforts to implement STIR/SHAKEN. However, neither Congress nor the FCC has set a deadline for implementing caller ID authentication. This bill does not prevent those efforts from occurring; instead, it sets a deadline by which caller ID authentication must occur. In the event that an FCC order or a federal statute that sets a conflicting deadline for implementation, the federal order or statute would likely preempt a state statutory deadline.

In 2016, the FCC convened a "strike force" consisting of representatives from the telecommunications and technology sectors to identify potential solutions to the illegal robocall epidemic. Implementation of STIR/SHAKEN was one of several recommendations proposed by the robocall strike force. In November 2017, the FCC adopted call-blocking rules that authorized telecommunications providers to aggressively block some types of robocalls. While the FCC has called for the implementation of STIR/SHAKEN by the end of this year, the commission has not adopted a specific regulation or order that would require the implementation of caller ID authentication. Instead, the FCC has required telecommunications providers to submit updates on their status of implementing STIR/SHAKEN. The reports show that some providers are implementing STIR/SHAKEN at a faster rate than other providers. By setting a deadline for implementation in California, this bill may encourage providers to ensure that they are implementing caller ID authentication in a timely manner. Providers that are already on track to complete implementation by the FCC's requested deadline will be in compliance with this bill as well.

Prior/Related Legislation

SB 1161 (Padilla, Chapter 733, Statutes of 2012) restricted the CPUC and other entities from exercising regulatory authority over VOiP unless expressly authorized or delegated to do so in law and strictly limits the scope of the authorization or delegation.

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

SUPPORT:

Area Agency on Aging Advisory Council
California Association of Competitive Telecommunications, support if amended
California Alliance for Retired Americans
Calsmallbiz
Consumer Attorneys of California, support if amended
Public Advocates Office

OPPOSITION:

AT&T
CTIA - The Wireless Association
California Cable & Telecommunications Association, oppose unless amended
Consolidated Communications Inc.
Frontier
Sprint
T-Mobile
Tracfone
Verizon

ARGUMENTS IN SUPPORT: According to the author:

> "Robocalls are the top consumer complaint in the nation. Despite attempts by federal agencies and Congress to prohibit illegal robocalls, the volume of illegal robocalls has increased. In 2017, Americans received over 30 billion robocalls, and experts estimate that between 30 and 40 percent of these calls were scams.
>
> While the FCC has urged telecommunications providers to adopt a system for preventing illegal robocalls, the FCC has not taken action to set a date by which providers must implement these systems.
>
> SB 208 is needed to establish a date by which telecommunications providers must implement caller ID authentication systems to ensure that California can effectively enforce consumer protection laws and take steps to limit these fraudulent calls."

ARGUMENTS IN OPPOSITION: Opponents argue that illegal robocalls should not be addressed at the state level, and efforts to comply with state-level requirements would detract from working with the FCC at the federal level to implement a national system. In opposition, CTIA states the following:

> Wireless carriers should be permitted to continue to focus on the important task at hand – implementing STIR/SHAKEN. Neither the California Public Utilities Commission nor the Attorney General is equipped to enforce laws dealing with robocalls. SB 208 will not hasten the process of implementing appropriate and necessary authentication technology. It will only divert attention and focus from that task and add a layer of CPUC regulation that is often obtuse and whose processes are lengthy and, certainly in this case, unnecessary.

-- END --