

The Florida Senate
BILL ANALYSIS AND FISCAL IMPACT STATEMENT

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

Prepared By: The Professional Staff of the Committee on Commerce and Tourism

BILL: SB 1516

INTRODUCER: Senator Garcia

SUBJECT: Caller Identification Information

DATE: February 10, 2026

REVISED: _____

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Renner	McKay	CM	Favorable
2.			RI	
3.			RC	

I. Summary:

SB 1516 regulates the transmission, authentication, and accuracy of telephone caller ID information in Florida.

The bill prohibits the transmission of misleading or inaccurate caller ID with the intent to defraud, cause harm, or wrongfully obtain anything of value. The bill requires telecommunications companies to provide the telephone number and originating location of each call and to block calls and text messages with manipulated caller ID information that doesn't match the telephone number or location. The prohibition does not apply to authorized law enforcement activity or a court order. The bill establishes civil penalties for violations up to \$250,000.

The bill defines the Secure Telephone Identity Revisited (STIR) and Signature-based Handling of Asserted Information Using toKENS (SHAKEN) authentication framework and requires telecommunications companies to implement such caller ID authentication protocols by July 1, 2027, with certifications filed with the Federal Communications Commission. The bill establishes civil penalties for violations up to \$250,000.

The bill does not appear to have a fiscal impact on state or local government agencies.

The bill provides an effective date of October 1, 2026.

Present Situation:

Federal Telephone Consumer Protections

National Do Not Call Registry

The Federal Trade Commission (FTC), in concert with the Federal Communications Commission (FCC), administers the National Do Not Call Registry.¹ Telephone solicitors may not contact a consumer who participates in the National Do Not Call Registry, unless the calls are:

- Made with a consumer’s prior, express permission;
- Informational in nature, such as those made to convey a utility outage, school closing, or flight information; or
- Made by a tax-exempt organization.²

The Truth in Caller ID Act³

Caller ID information that is altered to conceal the true identity of the caller and mislead the person receiving the call is referred to as “spoofing.”⁴ In response to the growing practice of spoofing, Congress amended the Telephone Consumer Protection Act⁵ to add the Truth in Caller ID Act of 2009 (Act). Under the Act and FCC rules, a person or entity is prohibited from transmitting false or misleading caller ID information “with the intent to defraud, cause harm, or wrongly obtain anything of value,” with a penalty of up to \$10,000 for each violation.⁶ However, spoofing is not illegal when no harm is intended or caused, or when the caller has legitimate reasons to hide their identity. Examples may include law enforcement agencies working on a case, a victim of domestic abuse, or a doctor who wishes to discuss private medical matters with a patient.⁷

Caller ID Authentication

The STIR/SHAKEN (Secure Telephone Identity Revisited and Signature-based Handling of Asserted Information Using toKENS) framework is a set of technical standards and protocols that allow for the authentication and verification of caller ID information for calls carried over Internet Protocol networks.⁸ In practice, calls traveling through interconnected phone networks can have their caller ID “signed” as legitimate by originating carriers and validated by other

¹ Federal Communications Commission, *Stop Unwanted Calls and Texts*, available at <https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts> (last visited Feb. 10, 2026).

² 47 U.S.C. § 227(a)(4); *See also*, 47 C.F.R. § 64.1200 (2012).

³ 47 U.S.C. § 227(e).

⁴ Congression Research Service, *Federal Communications Commission: Progress Protecting Consumers from Illegal Robocalls*, p. 1 (April 10, 2020). Available at

https://www.everycrsreport.com/files/20200410_R46311_fbb112c0038279f12c7ce63471c9eb5593945a67.pdf (last visited Feb. 10, 2026).

⁵ The Telephone Consumer Protection Act restricts the making of telemarketing calls and the use of automatic telephone dialing systems and artificial or prerecorded voice messages. *See* 47 U.S.C. § 227.

⁶ 47 U.S.C. § 227(e).

⁷ FCC, *Caller ID Spoofing*, <https://www.fcc.gov/consumers/guides/spoofing-and-caller-id> (last visited Feb. 10, 2026).

⁸ 47 CFR. §64.6301.

carriers before reaching consumers.⁹ Because the STIR/SHAKEN framework is only operational on IP networks, the FCC also requires providers using older network technologies to either upgrade their networks to IP or develop a caller ID authentication solution that works on non-IP networks.¹⁰

Florida Telephone Consumer Protections

Telecommunications Carriers

The Public Service Commission (PSC), an arm of the legislative branch of government,¹¹ ensures that Florida consumers receive utility services, including electric, natural gas, water, wastewater, and telephone, in a safe, affordable, and reliable manner.¹² To do so, the PSC exercises authority over public utilities in the following areas: rate base or economic regulation, competitive market oversight, and monitoring of safety, reliability, and service issues.¹³

Under ch. 364, F.S., telecommunications carriers in Florida are subject to limited PSC regulation. Telecommunications companies are defined to include every corporation, partnership, and person and their lessees, trustees, or receivers appointed by any court, and every political subdivision in the state, offering two-way communications service to the public for hire within the state by use of a telecommunications facility.¹⁴ The term *does not* include:¹⁵

- Entities that provide a telecommunications facility exclusively to a certificated telecommunications company;
- Entities that provide a telecommunications facility exclusively to a company which is excluded from the definition of a telecommunications company under this subsection;
- Commercial mobile radio service providers (mobile phone service provided for profit and to the public);
- Facsimile transmission services;
- Private computer data network companies not offering service to the public for hire;
- Cable television companies providing cable service as defined in 47 U.S.C. s. 522;
- Intrastate interexchange telecommunications companies;
- Operator services providers; or
- Airports that provide communications services within the confines of their airport layout plan.

⁹ FCC, *Combating Spoofed Robocalls with Caller ID Authentication*, available at <https://www.fcc.gov/call-authentication> (last visited Feb. 10, 2026).

¹⁰ *Id.*

¹¹ Section 350.001, F.S.

¹² See Florida Public Service Commission, *Florida Public Service Commission Homepage*, available at <https://www.psc.state.fl.us/> (last visited Feb. 10, 2026).

¹³ Florida Public Service Commission, *About the PSC: Overview and Key Facts*, available at <https://www.psc.state.fl.us/about#OverviewAndKeyFacts> (last visited Feb. 10, 2026).

¹⁴ Section 364.02(13), F.S.

¹⁵ Section 364.02(13)(a)-(i), F.S.

Florida Telemarketing Act

Chapter 501, part IV, F.S., the Florida Telemarketing Act (FTA), requires non-exempt businesses engaged in telemarketing and their salespeople to be licensed by the Florida Department of Agriculture and Consumer Services (DACS) before operating in Florida. Certain exempt entities must have a valid affidavit of exemption on file prior to operating in Florida. There are approximately 28 exemptions, including: soliciting for religious, charitable, political or educational purposes; research companies; newspapers; book and video clubs; cable television; and persons or companies with whom the consumer has a prior business relationship.¹⁶

The FTA generally requires businesses that solicit the sale of consumer goods or services to:

- Be licensed;¹⁷
- Post a form of security;¹⁸
- License all of their salespeople¹⁹ and
- Provide the DACS with a list of all telephone numbers used to make sales calls.²⁰

An application for licensure as a telemarketer must include several pieces of information, including the applicant's identifying information, prior experience in the field, criminal and administrative history (especially relating to fraud, theft, or unfair and deceptive trade practices), phone numbers from which the telemarketer will make sales calls, and any parent or affiliate entities under which it will transact business, if applicable.²¹

Call-Blocking Act²²

Under Florida's Call-Blocking Act, telecommunications companies that provide voice communications services to customers in Florida are authorized to preemptively block certain phone calls from reaching a customer's phone. In particular, consistent with federal law and FCC rules, such service providers may block calls:

- When the customer to which an originating number is assigned has requested that calls purporting to originate from that number be blocked because the number is used for inbound calls only.
- Originating from a number that is not a valid North American Numbering Plan (NANP) phone number.
- Originating from a valid NANP phone number that has not been allocated to a telephone service provider by the NANP Administrator or pooling administrator.²³

¹⁶ Section 501.604, F.S.

¹⁷ Section 501.605, F.S.

¹⁸ Section 501.611, F.S., requires a \$50,000 bond, irrevocable letter of credit issued for the applicant, or a certificate of deposit in favor of the DACS for payment on findings of fraud, misrepresentation, breach of contract, or other violation by the applicant.

¹⁹ Section. 501.607, F.S.

²⁰ Section 501.605(2)(k), F.S.

²¹ Section 501.605(2), F.S.

²² Section 365.176., F.S.

²³ A "pooling administrator" is defined as "the Thousands-Block Pooling Administrator as identified in 47. C.F.R., § 52.20." Thousands-block number pooling is a process designed to optimize the allocation of phone numbers. Under this process, 10,000 phone numbers are assigned to an individual geographic center and then split into 10 blocks of 1,000 numbers each. Each block can then be assigned to a service provider by a neutral number pooling administrator. See 47 C.F.R., § 52.20.

- Originating from a valid NANP phone number that has been allocated to a telephone service provider but is unused, if the provider blocking the calls: was allocated the number and confirms that the number is unused; or has obtained verification from the allocatee that the number is unused.

A service provider may not block a voice call from either of the first two categories listed above if the call is an emergency call placed to 911.

For purposes of blocking calls from certain originating numbers as authorized under the act, a provider may rely on caller identification service²⁴ information to determine the originating number.

While the Call-Blocking Act authorizes providers to block calls in specified scenarios, it is permissive and limited to scenarios consistent with authorization under federal law and FCC rules.

Caller-ID Spoofing

Pursuant to s. 817.487, F.S., a person is prohibited from entering or causing to be entered false information into a caller identification system with the intent to deceive, defraud, or mislead the call recipient. Additionally, a person may not make a telephone call knowing that false information was entered into the caller identification system with the intent to deceive, defraud, or mislead the recipient of the call. This does not apply to the blocking of caller ID information, to law enforcement agencies or federal intelligence agencies, or to telecommunications, broadband, or voice-over-internet service providers acting solely as intermediaries for the transmission of telephone service between a caller and a recipient. A person who violates this provision commits a first degree misdemeanor.²⁵

However, a U.S. District Court in Miami found that Florida's Caller ID Anti-Spoofing Act (2008) violated the Commerce Clause of the United States Constitution because it had the effect of controlling spoofing practices that took place entirely outside the state.²⁶ Similarly, in 2020, a federal court in North Dakota struck down North Dakota's anti-spoofing law, which was substantially similar to Florida's.²⁷

II. Effect of Proposed Changes:

Section 1 creates s. 364.242, F.S., prohibiting knowingly transmitting misleading or inaccurate caller ID information in connection with a telecommunications company. Telecommunication companies must provide the originating telephone number and location and must block all telephone calls and text messages with manipulated caller ID information that does not match the original number or location. This prohibition does not apply to transmissions in connection with

²⁴ "Caller identification service" is a service that allows a telephone subscriber to have the telephone number and, if available, the name of the calling party transmitted contemporaneously with the telephone call and displayed on a device in or connected to the subscriber's telephone. Section 365.176(2)(a), F.S.

²⁵ A first degree misdemeanor is punishable by up to one year in jail and a \$1,000 fine. Sections 775.082 and 775.083.F.S.

²⁶ *TelTech Systems, Inc. v. McCollum*, No. 08-61664-CIV-MARTINEZ-BROWN (S.D. Fla. Filed Oct. 16, 2008), 2009 WL 10626585.

²⁷ *SpoofCard, LLC v. Burgum*, 499 F. Supp 3d 647 (D.N.D. Nov. 9, 2020).

the authorized activity of law enforcement agencies or to court orders specifically authorizing the manipulation of caller ID information. The bill establishes \$250,000 civil penalties for violations of this provision.

Section 2 establishes s. 364.243, F.S., defining the STIR/SHAKEN authentication framework and requiring that all telecommunications companies adopt the STIR/SHAKEN authentication framework, or an equivalent technology that offers similar or enhanced capabilities for verifying and authenticating caller ID information on the company's Internet protocol networks, by July 1, 2027.

Telecommunications companies must file a certification with the FCC stating that their traffic is either digitally verified by the STIR/SHAKEN authentication framework or subject to a compliant automated call mitigation program. A copy of such certification must be provided to the Attorney General or the PSC upon request. The bill establishes \$250,000 civil penalties for violations of this provision.

Section 3 amends s. 365.176, F.S., to make conforming changes made by the bill, and specify that a provider may rely on information provided by the pooling administrator to deliver the originating number.

Section 4 provides an effective date of October 1, 2026.

III. **Constitutional Issues:**

A. Municipality/County Mandates Restrictions:

None.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

D. State Tax or Fee Increases:

None.

E. Other Constitutional Issues:

None identified.

IV. **Fiscal Impact Statement:**

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

Telecommunications companies may incur costs to implement or enhance STIR/SHAKEN protocols and compliance systems for authentication, blocking, and reporting.

Businesses and consumers may benefit from reduced fraud if caller ID manipulation diminishes; however, compliance costs and potential litigation could affect carriers.

C. Government Sector Impact:

Regulatory oversight and enforcement responsibility costs could be incurred and absorbed by the Attorney General or the Public Service Commission.

V. Technical Deficiencies:

None.

VI. Related Issues:

None.

VII. Statutes Affected:

This bill substantially amends section 365.176 of the Florida Statutes.

This bill creates sections 364.242 and 364.243 of the Florida Statutes.

VIII. Additional Information:**A. Committee Substitute – Statement of Changes:**

(Summarizing differences between the Committee Substitute and the prior version of the bill.)

None.

B. Amendments:

None.