Breaking Down The Expanded Reach Of Florida Caller ID Bills

By **Alexis Buese and Stephen Parsley** (February 23, 2026)

Alexis Buese

Stephen Parsley

In Florida's 2026 legislative session, both chambers are considering bills that would impose strict caller identification requirements on companies doing business in the state. S.B. 1516 and H.B. 1299 are framed as anti-fraud measures designed to combat robocalls and caller ID spoofing. But as drafted, they reach far beyond bad actors.

The legislation would affect any business that places calls or sends text messages to Florida consumers — including retailers, financial institutions, healthcare providers, mortgage servicers and consumer brands with national customer engagement platforms.

S.B. 1516 has been reported favorably by the Florida Senate Commerce and Tourism Committee, signaling meaningful legislative momentum. Companies with Florida consumer contact activity should be preparing for the possibility that this legislation will create new liability for their calling operations.

What the Bills Do

The proposed legislation would prohibit any person from causing a caller ID service to transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm or wrongfully obtain anything of value. The two bills target both telecommunications providers and the callers themselves.

Importantly, Florida already has an antispoofing statute. Under Chapter 817 of the Florida Statutes, Section 497, a person may not enter false information into a caller identification system — or knowingly place a call using false caller ID information — with the intent to deceive, defraud or mislead.

Violations constitute a first-degree misdemeanor. The statute does not apply to lawful caller ID blocking, law enforcement or federal intelligence agencies, or telecommunications and Voice over Internet Protocol providers acting solely as intermediaries.

The 2026 bills build on that framework but impose tighter operational obligations. Telecommunications providers would be required to authenticate caller ID information using STIR/SHAKEN protocols (or comparable technology), transmit correct phone number and location data, and block calls and text messages containing manipulated caller ID information.

While the bills do not expressly create a private right of action, Florida's aggressive consumer litigation environment cannot be ignored. Plaintiffs counsel may attempt to recast alleged violations as unfair or deceptive conduct under the Florida Deceptive and Unfair Trade Practices Act. The absence of a stand-alone private claim does not mean the litigation risk is minimal.

Why This Matters to Legal and Compliance Teams

For in-house counsel and compliance officers, the issue is not whether your company engages in fraudulent spoofing — it is whether your legitimate business practices could be swept into a broad statutory framework that does not clearly distinguish between fraud and operational reality.

Many multilocation retailers and financial services companies display a centralized customer service number regardless of where a call originates. Cloud-based phone systems and third-party dialers may use dynamic routing that causes the technical originating number to differ from the displayed number. Marketing campaigns may use campaign-specific callback numbers.

Under a strict interpretation of the bills, carriers could be required to block calls if authentication fails or if the displayed number does not match underlying transmission data. That means compliant business calls could be prevented from reaching consumers — creating operational disruption, reputational harm, and potential disputes with vendors and carriers.

The bill analysis acknowledges private-sector impact. Telecommunications companies may incur significant compliance costs to enhance STIR/SHAKEN authentication, blocking systems and reporting infrastructure. Those costs will not exist in isolation. They may be passed through contractually to enterprise customers.

At the same time, companies may face a second layer of risk: consumer complaints or litigation alleging that calls were blocked improperly, or that caller ID presentation violated state law. For companies already navigating the Telephone Consumer Protection Act, Florida Telephone Solicitation Act, mini-TCPA statutes and evolving consent standards, this adds another compliance variable.

Constitutional Considerations

Florida's prior antispoofing law has faced constitutional scrutiny.

In a case filed in 2008 — TelTech Systems Inc. v. McCollum — the U.S. District Court for the Southern District of Florida held that Florida's earlier Caller ID Anti-Spoofing Act violated the commerce clause of the U.S. Constitution because it had the practical effect of regulating spoofing activity occurring wholly outside the state.

Similarly, in SpoofCard LLC v. Burgum, the U.S. District Court for the District of North Dakota struck down a substantially similar statute in 2020.

If the new legislation reaches conduct occurring outside Florida — particularly in the context of nationwide calling platforms — it may invite renewed constitutional challenges. Companies operating nationally should be aware that patchwork state requirements affecting telecommunications infrastructure can create complex dormant commerce clause issues.

Practical Steps for Companies

Legal teams should be asking the following hard operational questions now:

- Do we use centralized or shared callback numbers across locations?

- Are our displayed numbers always technically consistent with the originating transmission data?

- Are we relying on third-party dialers or cloud systems that may not fully support STIR/SHAKEN authentication?

- What representations are in our vendor contracts regarding compliance and blocking risk?

- Are we prepared for potential service disruptions if carriers implement aggressive blocking?

If enacted, the law is expected to take effect Oct. 1, 2026 — a short runway for technical and contractual adjustments.

This legislation reflects a broader trend: States are layering additional compliance obligations on top of existing federal telemarketing and consumer protection regimes. For consumer-facing brands, caller ID compliance is no longer a narrow telecom issue. It is a litigation, operational and brand protection issue.

Companies that engage Florida consumers by phone or text should be monitoring these bills closely and coordinating across legal, IT, marketing and vendor management teams. Waiting until enforcement begins will be too late.

Alexis Buese is a partner and Stephen Parsley is an associate in Bradley Arant Boult Cummings LLP.