MARASHLIAN & DONAHUE, PLLC
THE COMMLAW GROUP

Federal & State Enforcement Agencies and Individual Plaintiffs are Aggressively Combatting a Single Concern: **Rampant Robocalls Using VoIP and Cloud Services**

The single most important step any company can take is to consult with experienced telecom counsel.

The *Comm*Law Group's "Robocall Mitigation Response Team" has the knowledge and experience of federal telemarketing law to help clients become and maintain compliant in the U.S. and internationally, identify risks, plan for cost-effective risk mitigation measures to support any defensive action, and red-flag issues surfacing in this rapidly changing federal, state, and local ecosystem.

Robocalling is a Hot Button Political Issue, and Every Candidate Wants a "Tough on Robocalls" Record!

State Attorneys General are aggressively pursuing Voice Service Providers (VSPs) for robocall violations, pushing compliance requirements, even beyond what the Federal Communications Commission (FCC) requires.

The most significant risk facing VSPs are the federal and state consumer protection policies and precedents being created through enforcement proceedings and litigation around robocall mitigation. Mitigating illegal and unwanted robocall traffic from your network, as a call originator or reseller, requires a gap analysis of your policies, practices, procedures, and tools.

Understand "Know or Should Have Known" Standards

The FTC's and some state AGs' robocall mitigation enforcement hinges on applying the "known or should ha known" standard to determine whether a provider facilitated an illegal robocall.

Telecommunications providers are expected to use the FTC's "Know Your Customer" (KYC) technology to ve identities of their customers before doing business.

Providers may be held liable for failing to utilize KYC technology to mitigate illegal robocalls.

1430 Spring Hill Road, Suite 310
Tysons, Virginia 22102
P 703.714.1300
E mail@commlawgroup.com
W CommLawGroup.com

U.S. Robocall Mitigation Ecosystem Demands All Telecommunications Companies Pay Attention as New Threats Emerge and Compliance Balloons Well Beyond Mere FCC Compliance

By The *Comm*Law Group

STIR/SHAKEN — Before you break out the martini glasses, this is not about the new James Bond film. Instead, this boozy-sounding acronym represents just one discrete element of broad Federal and state government-led effort to crack down on annoying (and often unlawful) telemarketing calls. If you were under the impression that implementing STIR/SHAKEN and complying with Federal Communications Commission (FCC) rules was all your communications company needed to avoid the crosshairs of government and private enforcement actions, think again!

Relieving American consumers of the tens of billions of nuisance calls, among the over 50 billion robocalls placed in 2021 alone, has become the "issue du jour" for not just the FCC, but also the Federal Trade Commission (FTC), Attorneys General from across the United States, and—wait for it—the class action plaintiff's bar.

Alongside STIR/SHAKEN, telecommunications carriers in the United States must now consider the broad, ever-expanding Robocall Mitigation ecosystem, representing a significant shift from traditional compliance centered on the FCC's regulatory landscape.

Perhaps the single most important step any company operating in the telecom business can take at this early and uncertain juncture is to consult with experienced telecom counsel. And not just any lawyer, but attorneys that possess both the knowledge and temperament to help clients identify risks and risk mitigation measures that will enhance their client's defensive positioning cost-effectively to ensure the cost of compliance doesn't overshadow the need to capitalize on business opportunities.

A New Telecommunications Ecosystem Centered Around Robocall Mitigation

As this ecosystem evolves and becomes more complex, providers must consider fluid, rapidly changing laws and regulations; government enforcement by the FCC and FTC; civil litigation; and the need to quickly respond to Industry Traceback Group (ITG) requests. Each represents a unique perspective and strategy for combatting a single concern: rampant robocalls deteriorating consumer trust.

FCC Compliance – A Valid Starting Point, but Insufficient Alone

Initially, the FCC required all telecommunications providers to comply with minimum requirements, including implementing STIR/SHAKEN or submitting a robocall mitigation plan (RMP) into the robocall mitigation database (RMD) by September 28, 2021 to ensure their calls aren't blocked. However, we see clear, unmistakable signs that compliance with the bare minimum FCC requirements — although a good starting point — will not be enough to satisfy the onslaught of government regulation and enforcement to come against the scourge of illegal robocalling.

In fact, we anticipate many voice providers, both big and small — and even some non-voice providers whose traffic is indistinguishable from voice — will find themselves ensnared in the grips of a multi-agency, multi-jurisdictional regulatory and enforcement ecosystem. Not to mention the potential for class actions from plaintiff's attorneys

relying on public sentiment to cast a wide Telephone Consumer Protection Act of 1991 (TCPA) net, ensnaring all providers in the call path, even intermediate carriers, associated with "bad" calls.

Even if FCC compliance is no longer sufficient, providers must make sure they stay up-to-date with and compliant with changes. The FCC continues to update requirements, such as a recent approval of public information collections associated with the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act, as the robocall ecosystem continues to evolve.

Failing to take actions, either through a "wait and see" approach or minimal compliance, could result in not only costs associated with damages or penalties, but increased compliance requirements with significant administrative and monetary burdens.

Ongoing FTC Regulatory Enforcement /// Understand "Know or Should Have Known" Standards for Customer Identity

While FCC compliance is relatively simple, recent FTC enforcement has shown the importance of "Know Your Customer" (KYC). As the name might suggest, companies use KYC to verify the identities of their customers before doing business. Telecommunications providers can — and are expected to by the FTC — use KYC to ensure that no illegal robocalls are going through to consumers.

After all, the FTC's enforcement of providers' facilitation of illegal robocalls hinges on the "known or should have known" standard. Essentially, telecommunications providers may be held liable for failing to utilize KYC technology to mitigate illegal robocalls.

In 2019, the FTC alleged that defendant Globex Telecom, Inc. assisted and facilitated telemarketers it knew, or consciously avoided knowing, were violating the Telemarketing Sales Rule's prohibitions on calls delivering prerecorded messages. FTC v. Educare Centre Services, Inc., No. 3:19-cv-00196-KC (W.D. Tex. Am. Compl. filed Dec. 3, 2019). The Court halted Globex's Voice over Internet Protocol (VoIP) services pursuant to a Temporary Restraining Order, showing the significant and immediate impacts to businesses subject to federal regulatory enforcement. In 2020, the FTC sent a warning letter about facilitating illegal robocalls that referenced the Educare case to an intermediate carrier. If the intermediate carrier had engaged in KYC, the warning might have been avoided.

Emerging Threats to the Status Quo of Telecommunications Enforcement // AG's

In addition to regulatory enforcement by the FCC and the FTC, additional threats to telecommunications providers are likely to come through enforcement actions by state attorneys general (AGs) and even civil litigation initiated by private parties.

For example, state AGs have begun to sue under state consumer protection and deceptive marketing statutes, in part because of growing public frustration with nuisance robocalls. This patchwork of litigation and enforcement could lead to state-by-state compliance. However, state AG enforcement will likely be consistent, including both monetary penalties and forced implementation of technical solutions and processes to combat robocalls. Providers must be aware of nuanced state requirements that impact their services—not knowing what applicable state consumer protection standards might impact your business makes it virtually impossible to know if they are violated until a notice letter is sent when implementing KYC is often too little too late.

Proactively implementing appropriate KYC, following FCC rules, and understanding applicable nuanced state requirements with the help of experience telecommunications counsel can pay significant dividends: reducing the

likelihood of penalties and forced compliance that, in retrospect, is likely overkill and much more than would have avoided the issue initially.

// + Private Litigation

Growing civil litigation by private plaintiffs presents a greater unknown, both in terms of enforcement strategy and consequences, than even rapidly evolving federal and state enforcement. This shift to increased private litigation represents both the growing public frustration and desire by plaintiffs to protect their interests where potential significant recovery exists. In fact, plaintiffs are already alleging damages up to the TCPA's statutory maximum–$500 per call or $1,500 if conduct was willful—against all providers in the call path. For intermediate providers making fractions of a cent in profit, proactive compliance measures are a smart, cost-effective way to avoid these potential damages and litigation expenses.

Such litigation represents a recurring theme: wherever the legal ecosystem evolves, providing the opportunity to recover damages, class action plaintiff's lawyers and attorneys for large enterprise consumers of voice services, such as call center operators, are certain to seize upon those opportunities.

We anticipate that questions around the meaning of and extent to which the "Know Your Customer" requirements apply in different contexts will ultimately be answered through litigation and enforcement, and less so through the FCC regulatory rulemaking process, which will lag, particularly as consumer frustrations reach a boiling point.

Questions around damages and who is or can be held responsible for originating, passing, or terminating illegal robocalls are also going to be fleshed out by regulatory enforcement and private litigation. This real, looming threat will affect providers of all sizes, who must be aware of them and factor in risk tolerance to determine what compliance efforts and proactive steps are appropriate.

Unprepared telecommunications providers—likely those with the worst or lowest compliance—will be left holding the bag, which they will need to fill with significant settlement funds.

Ongoing Private Enforcement Shows Some Strategies Being Implemented

Last year, Marriott filed a federal lawsuit against "John Does" alleging, among other harms, illegal robocalls misusing Marriott's name and violating its intellectual property rights. We speculate that the use of "John Does" preserves Marriott's ability to amend its complaint to implead carriers and providers that carried or transported the fraudulent traffic. Further, Marriot can rely on the FTC's "known or should have known" standard to show underlying carriers are the "John Does" that profited from bad actors.

In an unrelated case, a plaintiff suing on behalf of a proposed class argued that several defendants violated federal law for making "obviously spoofed robocalls" carrying pre-recorded or live scam messages using an automatic telephone dialing system. Notably, the court rejected motions to dismiss, rejecting defendant's arguments that they were "mere middlemen" transmitting the call, showing the significant risks to all telecommunications providers, including originating, intermediate, and terminating carriers.

Ongoing Revisions to Consumer Protection Laws Further Complicate Compliance and Increase Risks

To summarize, let's take a look at what "Rules of the Road" apply beyond the FCC's regulations.

First, the most significant risk—even more so than the FCC—are the federal and state consumer protection laws being developed around robocall mitigation. Voice Service Providers (VSPs) should start with the FTC, where the strict "known or should have known" standard is applied to hold VSPs accountable for illegal robocallers using their networks; VSPs should therefore work actively with intermediate and terminating carriers to mitigate illegal robocalls and help prevent those carriers inadvertently blocking the VSPs' calls.

Next, the same expectations—via KYC and the FTC's "known or should have known" or a similar standard—are likely to be applied by state AGs enforcing local consumer protection laws to protect their citizens.

And from there? You got it! It's only a matter of time until the standard of care is being fleshed out in courtrooms all across the country, particularly in private suits where creative attorneys craft cutting edge legal arguments relying on any and all possible standards.

Telecommunications Providers Should Proactively Seek Advice from Counsel to Address Issues Today and Avoid Significantly Higher Costs and Compliance Requirements in the Future //

Hire us so you do not fall into one of these crazy holes that are popping up because there is no precedent yet!

You don't want to be a guinea pig. Things are uncertain. You need someone monitoring developments and keeping your business apprised of developments that may impact your bottom line!

While it pays off to keep your ear to the ground and pay attention to the entire ecosystem, enlist the support of legal counsel that has telecom experience and a robocall mitigation team—experts that understand this evolving ecosystem and can guide you, not matter your stage in compliance or litigation. A trusted legal advisor can ensure you stay in the loop, update and pivot as needed, and guide your compliance efforts to ensure you are informed and within a comfortable risk exposure.

Companies can be proactive or reactive. Proactive companies that engage counsel early will stay off the radar and timely resolve issues with tools, contracts, policies, and procedures. Reactive companies will save today but pay significantly—both in terms of time and money—to put out fires that could have been avoided.

Reflecting on the history of these types of massive, earth-changing regulatory movements, our Magic 8-Ball tells us that lawyers will be busy defending clients on robocall-related disputes in the future. When it comes to operating in the new ecosystem created by the national effort to curb illegal robocalling, be sure to spend your money wisely, but avoid sitting on your hands and ducking your head in the sand because doing so will come at a remarkably high (and yet entirely avoidable) price.

If you are in the market for legal counsel to guide you through this uncertain time, look no further. The CommLaw Group has the expertise and focus to help telecom providers everywhere assess their risks and bring them within their tolerance. We can assist with assessing compliance, evaluating KYC, and drafting appropriate contracts. But, more importantly, we are aware of the evolving ecosystem and associated risks involved in the national (and at times very local) war against robocalls.

NEED HELP WITH ROBOCALL MITIGATION, COMPLIANCE AND LITIGATION SUPPORT/DEFENSE AGAINST BUSINESS & LEGAL CHALLENGES?

The *Comm*Law Group Can Help!

Given the complexity and evolving nature of the FCC's rules, regulations and industry policies & procedures around Robocall Mitigation and Compliance issues (e.g., Stir/Shaken, TRACED Act, FCC Rules & Regulations, US Telecom Industry group, ATIS, NECA, VoIP Numbering Waivers, Know Your Customer and the private sector ecosystem), as well as the increased risk of business disputes, consumer protection enforcement by state attorneys general, and even civil litigation, and anticipating the potential torrent of client questions and concerns, The CommLaw Group formed a "Robocall Mitigation Response Team" to help clients (old and new) tackle their unique responsibilities.

CONTACT US NOW, WE ARE STANDING BY TO GUIDE YOUR COMPANY'S COMPLIANCE EFFORTS

Rob Jackson
REQ@CommLawGroup.com

Michael Donahue
MPD@CommLawGroup.com

Ron Quirk
REQ@CommLawGroup.com

www.CommLawGroup.com

703-714-1300

ATTORNEY ADVERTISING DISCLAIMER: This information may be considered advertising in some jurisdictions under the applicable law and ethical rules. The determination of the need for legal services and the choice of a lawyer are extremely important decisions and should not be based solely upon advertisements or self-proclaimed expertise. No representation is made that the quality of the legal services to be performed is greater than the quality of legal services performed by other lawyers.