

Half Year 2026 Robocall Investigation Report

By Transaction Network Services

July 2026

Executive Summary

STIR/SHAKEN is working where it is fully deployed — but TNS data shows bad actors are now exploiting the uneven parts of the voice ecosystem.

After nearly three years of full enforcement, the industry has achieved strong results, yet persistent gaps continue to erode subscriber trust.

Top Takeaways

- **The largest Communications Service Providers (CSPs) are holding steady:** The top seven have stabilized around **85%** signed inter-carrier traffic, the vast majority with "A" attestation.
- **The non-top-tier remains exposed:** Smaller CSPs hover at **19–20%** signed traffic terminating to their networks, with only single-digit movement and occasional regression.
- **"A" attestation does not automatically equal trust:** TNS data points to around **10–12%** of Verstat-passed traffic being tagged unwanted and **17%** of confirmed spoofed calls carrying "A" attestation.
- **VoIP remains a disproportionate source of unwanted traffic:** VoIP lines continue to drive an imbalanced share of spam and show worsening performance in key metrics for non-top tier CSPs.
- **AI is raising the stakes:** Scams are becoming personalized, multimodal, and convincing through deep-fake voice cloning and sophisticated bypass tactics such as SIM boxing.

These disparities underscore the robocall compliance environment today. Mandated under the TRACED Act and phased in from 2021–2024, the STIR/SHAKEN framework required significant upgrades. While asset-class top-tier CSPs delivered, many smaller CSPs with limited resources continued relying on minimal compliance and legacy TDM/SS7 interconnects that stripped signatures and broke the chain of assurance.

High-risk scam calls keep surging in effectiveness. TNS observed targeted and multimodal campaigns that combine voice and text to pressure victims into clicking, calling back or making payments.

Fraudsters are harvesting target lists, prioritizing victims and supercharging millions of calls with AI-optimized scam scripts.

TNS data — drawn from more than 1.5 billion daily call events across 150+ CSPs and nearly 300 million subscribers — clearly shows both the progress at the top and the systemic vulnerabilities from below.

TNS solutions are designed to directly address these challenges: TNS Hosted Cloud Connect for legacy/IP migration, TNS Call Guardian for attestation and reputation weaknesses, Enterprise Branding and Call Authentication for contact center exposure, and AI-powered tools to combat deepfakes and advanced scams.

The long process of compliance implementation has hit its stride for the leading CSPs. The industry must now close the gaps through modernization and layered defenses to continue to restore trust in voice communications.



Key Findings

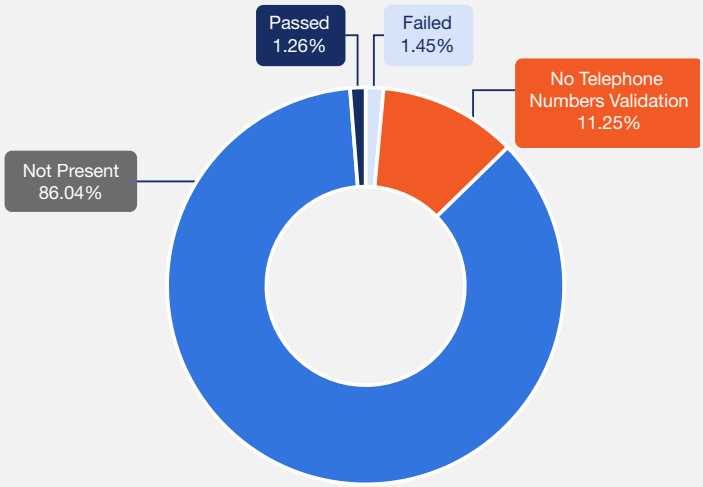
Though STIR/SHAKEN has come of age, AI-enabled fraudsters keep raising the bar. With this Half-Year Robocall Investigation Report, TNS is committed to helping decision-makers stay ahead of the curve.

Compliance data for the first half of 2026 reveals incremental progress at the industry's highest echelons alongside persistent trust challenges for the non-top-tier.

If they haven't already, this means that many smaller CSPs face real cost, infrastructure and migration challenges. Data shows their networks are increasingly exploitable, making practical modernization and layered mitigation urgent.

As compliance adoption evolves and legacy TDM reaches end-of-life, the message is clear: regulators are enforcing the rules and telecom decision-makers must accelerate migration to cloud-native networks. The integrity of the voice channel is at stake.

Invalid Telephone Numbers by Verstat





> **Top CSPs have plateaued at a high level of performance enabled by full IP infrastructure, while non-top tier CSPs lag due to legacy dependencies," said John Haraburda, TNS Director of Product Management. "This is not unexpected three years post-mandate, but continued stagnation risks further industrywide erosion of subscriber trust."**

Robocall Performance: Plateau at the Top, Lag Below

Top-tier CSPs maintain strong performance with approximately 85% of inter-carrier traffic predominantly signed with "A" attestation. This level has held steady since late 2023, demonstrating the maturity of SIP-to-SIP connectivity among the leaders. When signed, over 90% of traffic originating between these CSPs is Verstat-passed.

Non-top tier CSPs, however, hover at 19-20% signed traffic terminating to their networks; a figure that has shown only single-digit improvement and occasional regression over the last few years.

Much of the shortfall stems from TDM/SS7 hops that strip STIR/SHAKEN signatures, combined with limited direct SIP peering to top-tier CSPs.

VoIP-originating traffic exacerbates the issue, arriving unsigned or improperly attested at higher rates. Invalid numbers [unallocated, Do-Not-Originate (DNO), not-in-use] receive "A"/Verstat-passed attestation in roughly 1.6% of observed cases, while 10-12% of Verstat-passed traffic is still tagged unwanted. TNS Enterprise Branded Calling (EBC) data shows 17% of confirmed spoofed calls arriving with "A" attestation and 13% arriving unsigned.

Wireless and wireline traffic to non-top tier CSPs also shows elevated unwanted percentages compared with top CSPs.

Attestation Trust and Over-Attestation Issues

Improper attestation remains a core concern. Though statistically few against total volume, incoming calls with spoofed labelling is a problem and too much traffic from invalid numbers is still arriving with "A" attestation and Verstat-passed.

STIR/SHAKEN can confirm that a call is signed, but it cannot determine every dimension of call intent, reputation or legitimacy. That is why analytics, reputation scoring and spoof protection are important.

Among calls blocked via the TNS Branding and Call Authentication Suite, which includes Spoof Protection, 17% carried "A" attestation. Even when Verstat-passed, 10-12% of traffic is tagged unwanted by TNS analytics. Rich Call Display (RCD) claims show similar challenges, reaching as high as 27% of certain RCD-labeled traffic rated as unwanted.

As the volume of improperly attested calls grows, trust in voice communications may decline, even when consumers experience only a few illegitimate calls that are incorrectly signed as authentic arrive without warnings.

These findings reinforce that attestation alone is not a silver bullet. Originators can over-attest and exploit gaps. For reliable trust, downstream CSPs and enterprises need layered analytics, reputation scoring, spoof protection, invalid-number interrogation, and out-of-brand verification (branded calling, voice biometrics).



Unwanted Traffic Patterns by Line Type and Carrier Class

High-risk and nuisance calls remain elevated in VoIP segments, which continue to drive spam despite lower overall volume share.

Non-top tier CSPs see significantly high unwanted percentages across wireless/wireline and especially VoIP traffic, often 9x the relative burden in certain unwanted categories compared with the seven top-tier CSPs. SIM box fraud incidents are on the rise, with fraudsters routing internal-looking "A"-attested traffic through gateway farms to bypass controls.

AI supercharges fraudsters' sophistication: voice cloning appears in high-risk incidents, and multimodal (voice + text) attacks are increasing.

The following AI-generated robocall voicemail script is targeted and personalized to business owners and financial managers. It was followed by a series of texts that phished for a click or a callback:

"It's Barbara calling again. I have you pre-approved for an up to $308,000 business credit line. We just need a few verifications to finalize, so press one or call me back. We can have the funds wired to your account as soon as tomorrow."

Fortunately, anti-fraud tools are proving effective where they are deployed. For example, TNS Call Guardian continues to deliver strong mitigation through reputation scoring, anomaly detection and SIM-box identification.

Regulatory and Industry Response

The FCC continues advancing enforcement and proposed rulemakings, which are focused on non-IP vulnerabilities, "Know-Your-Upstream-Provider" diligence, and stricter attestation accountability.

Regulators removing errant CSPs from the Robocall Mitigation Database persist, creating severe financial pressures for the non-top-tier especially, and for all CSPs that touch unwanted traffic. Smaller, non-top-tier CSPs face rising compliance costs and operational jeopardy if they remain at minimal levels.

TNS Solutions Address the Gaps

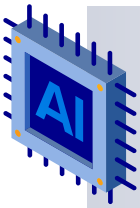
Scams are becoming targeted, believable and scalable. AI-enabled TNS detection and security solutions are purpose-built to meet the specific challenges highlighted throughout this report.



Legacy infrastructure limits signing and creates interconnect gaps. **TNS Hosted Cloud Connect** supports TDM-to-SIP migration.



"A" attestation is not enough. **TNS Call Guardian** adds reputation scoring, anomaly detection and spoof protection.



TNS AI-enabled tools help combat deepfake and advanced scam attacks. These solutions include AI-powered voice biometrics, predictive call analytics and generative AI capabilities that help CSPs stay ahead of increasingly sophisticated multimodal and voice-cloned attacks.

Together, these offerings help CSPs of all sizes work to reduce legacy dependency and compliance risk, strengthen attestation trust, help protect enterprises and support modernize networks.

Nothing stands still," said Seth Walton, General Manager, TNS Communications Market.

"By embracing continuous improvement, the entire industry can build a resilient environment where trust endures, no matter how the threat landscape evolves."

Scams Overview

Scammers in the first half of 2026 moved quickly, leveraging AI tools to make their attacks convincing and personalized. Here are some of the top scams TNS has been tracking:

World Cup / Ticket Scams

Fraudsters flooded networks with robocalls and texts offering fake 2026 World Cup tickets, resale deals, and "official" hospitality packages.

Vulnerable fans were targeted, especially during the spring qualification and early tournament excitement. Scammers used AI-generated voices impersonating athletes or organizers to create urgency with call-to-action scripts, such as:

"This is a limited availability offer – buy now before they sell out."

Victims were directed to phishing sites for payment or asked to provide credit card details over the phone. These scams matter because they demonstrate how bad actors exploit major global events, blending robocalls with smishing to pressure fans into quick, emotional decisions.

Utilities Scams

Impersonators posing as local utility companies called subscribers warning of imminent service shutoffs due to "billing errors" or "meter problems." Seniors and fixed-income households were primary targets. The calls used spoofed local numbers and high-pressure language such as:

"Your power will be disconnected in 30 minutes unless you pay $289 immediately via gift card."

Victims were instructed to buy the cards and read the numbers over the phone. These kinds of scams create immediate panic around essential services, leading to rapid financial loss before victims can verify the claim.

Government Agency Impersonation Scams

A sharp rise occurred in calls spoofing DMV offices, sheriff departments, and other agencies claiming outstanding warrants, unpaid tickets, or urgent legal matters. Working-age adults and elderly residents were heavily targeted.

Scammers used official-sounding AI voices and spoofed government numbers, demanding immediate payment to "resolve" the issue and avoid arrest. Typical script:

"This is Officer Ramirez with the county sheriff's office. There is a warrant for your arrest related to an unpaid traffic violation. Pay $450 now or we will send a unit to your home. These types of scams are effective because they weaponize authority and fear, making victims likely to comply without checking legitimacy.



Ghost Tax Preparers

During tax season, fraudsters spoofed numbers to impersonate IRS agents or offered "fast tax preparation" services. Busy professionals and elderly filers were primary targets.

Many calls claimed that large refunds were ready but required a small "processing fee" or bank details to release funds with scripts like this:

"Hello, this is David from Elite Tax Solutions. We've been reviewing your 2025 tax return and found you're eligible for an additional $2,847 refund that wasn't claimed. We just need to verify your banking information and process a small $89 filing fee. Press one now."

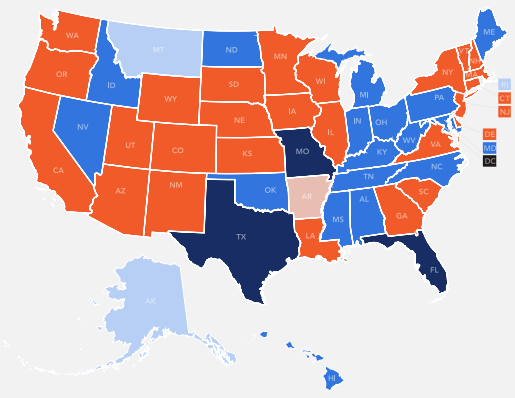
Others posed as legitimate preparers who could "fix" returns for a fee. This approach illustrates the danger of cyclical scams, in this case striking at a time of year when people are focused on finances and willing to share sensitive information.

Friendship Scams

Bad actors used advanced voice cloning to impersonate family members or close friends. Elderly subscribers were the main targets. Many campaigns began with an emoji-laced text:

"Happy birthday, boo. I hope you are enjoying your birthday trip. We need to celebrate together when you get back."

This was followed by a cloned voice call requesting emergency money for a fake medical issue or travel problem. These scams exploit personal trust and emotion, often resulting in large transfers before victims realize the voice was synthetic.



Top Scams of 2026

- Donation
- Financial Services
- Government
- IRS
- Job Offer
- Prison Call Payment

Award Recognition

The TNS Enterprise Branding and Call Authentication Suite continues to gain industry recognition for helping enterprises turn trusted voice engagement into a competitive advantage. Named a **Platinum winner by Juniper Research in both the Robocall Mitigation and Branded Calling** categories, the suite demonstrates the power of combining call authentication, brand presentation and fraud protection into a single, enterprise-ready solution. TNS also earned a **ChannelVision Visionary Spotlight Award in the Contact Center/CCaaS** category for helping contact centers verify legitimate calls, mitigate spoofed traffic in real time and give customers more data so that they can have greater confidence when deciding to answer a call. Together, these honors reinforce TNS leadership in restoring trust to outbound communications, protecting brand reputation and helping enterprises connect with customers when every answered call matters.

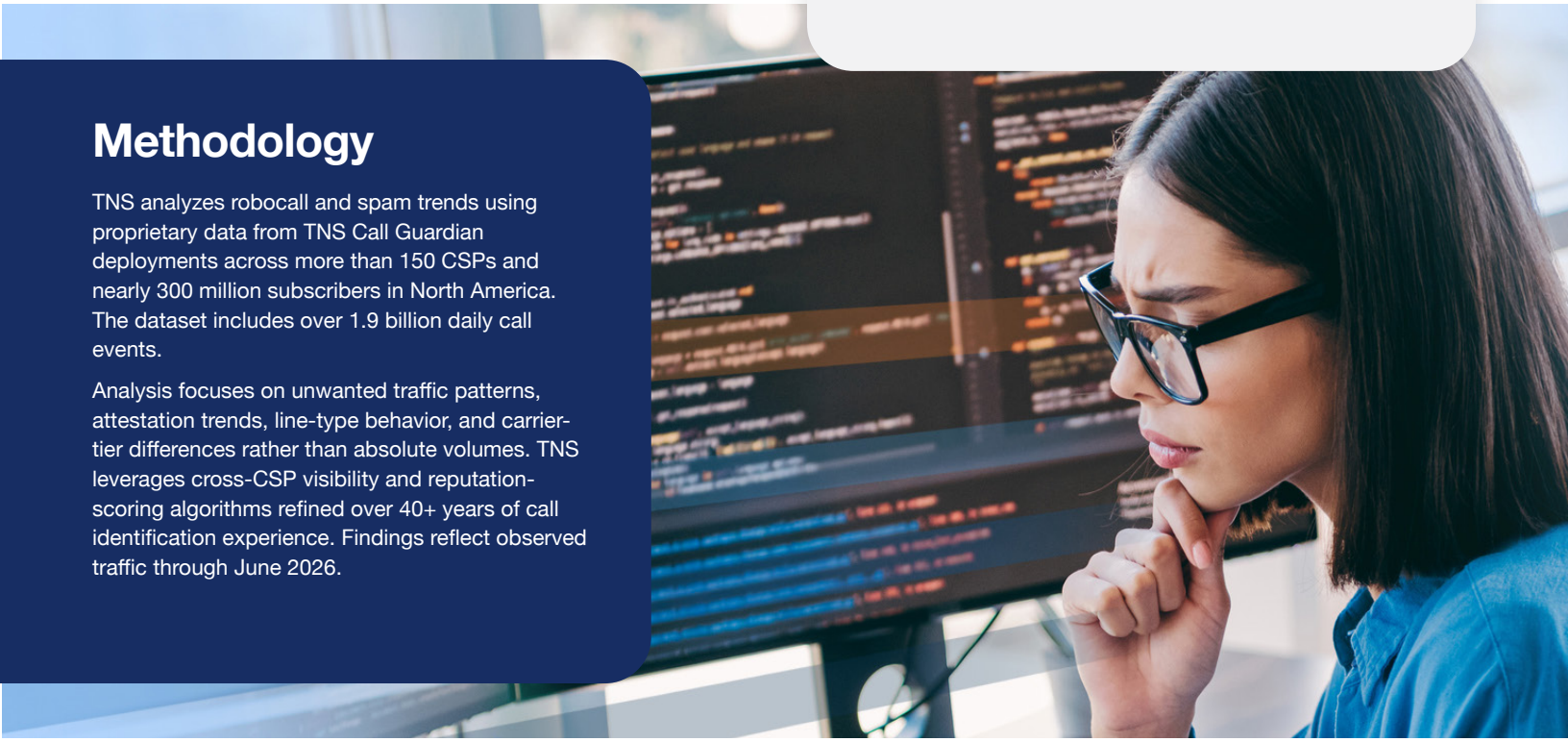
Future Digital Awards

2026 VISIONARY SPOTLIGHT AWARDS CHANNELVISION WINNER

Methodology

TNS analyzes robocall and spam trends using proprietary data from TNS Call Guardian deployments across more than 150 CSPs and nearly 300 million subscribers in North America. The dataset includes over 1.9 billion daily call events.

Analysis focuses on unwanted traffic patterns, attestation trends, line-type behavior, and carrier-tier differences rather than absolute volumes. TNS leverages cross-CSP visibility and reputation-scoring algorithms refined over 40+ years of call identification experience. Findings reflect observed traffic through June 2026.



To learn more about TNS's robocall protection services please visit:

tnsi.com/solutions/communications/robocall-protection/
or to request a copy of our annual full year Robocall Investigation Report please visit tnsi.com/resource/com/tns-robocall-investigation-report/

©2026 Transaction Network Services. All rights reserved. The information contained within this document is the confidential information of Transaction Network Services. Disclosure, distribution or use of this document is not permitted outside of Transaction Network Services without written permission. Subject to non-disclosure obligations of Transaction Network Services employees and contractors.

Call Guardian is a registered trademark of Transaction Network Services, Inc.