Third Quarter Robocall Investigation Report

By Transaction Network Services

October 2024

Executive Summary

During the third quarter of 2024, dramatic political events gave scammers the opportunity to try new tactics for political robocalls – and it's not over yet. TNS continues to track at least a doubling of unwanted calls and illegitimate activity around significant events:

- **The Donald Trump vs. Joe Biden debate in June**
- **The Donald Trump assassination attempt and Republican Convention in July**
- **The Democratic Convention in August and election-season kickoff after Labor Day**
- **The Kamala Harris vs. Donald Trump debate and second Donald Trump assassination attempt in September**

Political Robocall Data

There have been major surges in North Carolina, Michigan and Arizona. For example, North Carolina went from tens of thousands to hundreds of thousands of calls per week during a three-week streak in August. Though Michigan has been in the top ten states nationwide as far as spam traffic, what is concerning is that even with this volume of traffic, Michigan has yet to hit the high-water mark in a single week at the peak of its primary contest.

With what we've observed throughout the year, and what we know we can expect, the anticipation during this final stretch is palpable. The bottom line for carriers is that customer trust in the voice channel remains at risk.

TNS saw general robocall traffic ramp up significantly in September. During the second half of the month, the top states for political robocalling were:

- **Arizona**
- **Michigan**
- **New Hampshire**
- **Nevada**
- **Wisconsin**

High volumes are expected to continue into October with political spam prevalent in the following states and collectively representing over 60% of nationwide spam:

- **Arizona**
- **Minnesota**
- **North Carolina**
- **Pennsylvania**
- **Wisconsin**

Arizona, Michigan and Pennsylvania have ranked consistently high over the entire election season. Though North Carolina has been decreasing (with disruptions due in part to Hurricane Helene), new states, like Nevada, have joined the top rankings. With its low population but potentially contentious senate race, Montana has been clocking high. On the other hand, some states have remained consistently low in the rankings of political robocalls per capita:

- **Alabama**
- **Alaska**
- **California**
- **Hawaii**
- **Texas**

Other states have presented marked decreases in spam calls during election season, most likely due to foregone conclusions about voters' decisions on certain candidates:

- **Connecticut**
- **Minnesota**
- **New Mexico**
- **Utah**
- **West Virginia**

Though there has been essentially a doubling of spam calls over the third quarter, there is less total volume than initially anticipated at the end of the first half of the year. In forecasting the final run-up, we're still expecting major spikes in the hotly contested states and a nationwide ramp-up in political robocalls across the board. Since the beginning of October, we've seen the anticipated spike in political spam calls. In fact, the volumes have spiked by over 300% since October 1.

Types of Political Scams

TNS' Robocall Protection team has tracked an increase in unwanted political calls this year. Adding to the frustration, many of the calls and texts coming from campaigns, parties and pollsters are legal.

The key to maintaining customer confidence is to empower subscribers to make informed decisions on which legitimate calls to answer. To increase those answer rates, carriers need to understand how to detect and properly sign political scams despite clever bad actors who appear to be following legal robocall rules.

What's Legal?

Auto-dialed or pre-recorded political calls are allowed to contact landlines without prior consent. However, they are limited to three calls per month, and anyone on the receiving end can revoke consent at any time.

For cellular and internet-connected devices, political parties and campaigns are not permitted to auto-dial or send pre-recorded robocalls without the receiver's consent. The caller's name or the representative entity must be provided at the start of the message and their telephone number must be signed at the beginning or the end of the message.

Text messages follow the same guidelines. The FCC encourages users to report unwanted calls and texts, and to let regulators and law enforcement know if they believe their phone number is being spoofed, blocked or labelled as possible scam.

How To ID Political Scams

More challenging than ever before, the distinctions between unwanted and legitimate calls remain unclear to consumers. Following STIR/SHAKEN protocols, carriers need to both authenticate real calls and accurately identify suspicious activity, especially the many scams becoming more prevalent during elections.

False fundraisers using robocalls and AI-generated scripts are the easiest to spot. Scammers pretending to raise money for a campaign or a candidate will ask for a donation, pocket the cash, then disappear.

Subscribers should be advised to never give personal, bank card or monetary information of any kind over the phone, especially to unsolicited or unfamiliar callers. For anyone wanting to make a donation to virtually any organization, it's best to go directly to a verifiable website.

Plenty of legitimate robocall campaigns are successfully referring voters to real sites. However, there are also plenty of fake sites that can easily confuse and suppress voters and steal their money. Fly-by-night scammers often deploy temporary sites, target victims, then take them down quickly to avoid detection.

AI Voice Cloning

Unfortunately, as AI-generated robocall theft evolves, scams are sounding more believable. Fraudsters have easy access to legal voice cloning tools that can convincingly impersonate familiar voices and are capable of conducting actual conversations. The quick giveaway is when a synthetic voice asks for personal information directly over the phone.

Voter Fraud

In addition to fundraising scams, actual voter fraud is becoming far more common. An illicit robocall may claim the target can vote over the phone, for which they'll need to impart personal information, such as name, address and Social Security number.

The scammers' goals can be twofold: to gain personal information and/or to spread misinformation to keep people away from polls so they won't vote for an opposing candidate. For instance, the caller may recommend voting the day after the election to avoid anticipated long lines at the polls.

Nowhere in the United States is voting done over the phone, so any attempt to do so is an immediate red flag. Again, these can be both financial crimes and illegal acts of voter suppression that can be prosecuted under federal law.

Both landline and wireless subscribers should be encouraged to avoid falling victim to various forms of voting scams by checking when and where to vote with their state, county and municipal election departments.

Especially over the last quarter, subscribers are wising up and not answering unknown numbers at all. With more frequency, they're also reporting suspected scams, nuisance and unwanted calls to their carriers.

In addition, it's important to encourage vigilance in notifying local police, state attorney general offices, and the Federal Trade Commission (FTC). State and federal election authorities are getting more involved as well with the increase in fraudulent robocalls being used to confuse and suppress voters.

Call-blocking apps, such as those powered by TNS Call Guardian®, are excellent resources for reporting and blocking unwanted robocalls. The latest information about scam techniques is available on TNS' monthly Scam of the Month page.

AI Trends

Sinister deepfakes have been making headlines since earlier this year when an AI-generated voice audio of President Joe Biden was sent to democratic voters' phones urging them not to vote in the New Hampshire Primary. In response, the FCC took quick action and outlawed robocalls using AI-generated voices.

Despite the fact that these calls were traced to their original source and criminal charges were made in the New Hampshire incident, fraud and suppression attempts like this are growing virtually unchecked around the world. In Slovakia, for example, AI-generated audio of a well-known party leader was used in a robocall that claimed the election was rigged just before voters went to the polls.

The TNS anti-fraud decoy network lures in robocalls using a honeypot of inactive or out-of-service telephone numbers. We're seeing legitimate get-out-the-vote (GOTV) calls that will often use a script like this:

> **"Hello, this is Chairman Evan Power calling on behalf of the Republican Party of Florida with an important message. Our records indicate that your vote-by-mail ballot request may have expired due to a recent update in state law. You can renew your vote-by-mail ballot request today by visiting RepublicanRenewal.com."**

Unfortunately, illegitimate robocalls are becoming far more frequent and are harder to distinguish from legitimate calls. Typically, the scam's call to action will take the target to a fake website.

Here's an example of an AI-generated scam script that attempts to start a rudimentary conversation with the victim. The goal is to get them to go to a fraudulent site to reveal their personal information and/or be shown misinformation to suppress their vote:

> **"Hello, Yvonne."**
>
> **"Hi..."**
>
> **"Our records show that you're not registered to vote at your current address."**
>
> **"Okay...."**
>
> **"Would you like to register so you can vote in November? Just go to our website where you can register and vote online. It only takes two minutes."**

Political Robocalls Subscriber Survey Data

TNS commissioned research firm KANTAR to conduct an independent survey of US consumers to gain real-time insights into opinions on political robocalls.

More than 1,000 adults aged 18 to 64 were surveyed during the lead-up to the presidential election. The research identified public sentiment regarding the role of AI in campaigns and how consumers should be warned and educated of potential scams.

The most significant takeaway from the survey is that awareness is high: More than 70% of Americans are concerned about AI deepfake robocalls. Nearly two-thirds (64%) believe deepfake robocalls can be convincing enough to impact the outcome of the presidential election itself.

The data was released in a new TNS eBook: America Votes – 2024 US Presidential Election in Robocalls detailing near-universal fears of both foreign and domestic bad actors interfering in elections.

Key data narratives emerging from the survey include:

60% of Americans believe robocalls and robotexts are being used to undermine confidence in the 2024 presidential election.

71% believe voters in battleground states are more likely to be targeted by an AI deepfake robocall attempt than voters in non-battleground states.

67% believe the differences between legitimate election robocalls and those containing false information are often unclear.

77% agree that policymakers, regulators, network operators and solutions providers should educate Americans on the risks of political AI deepfakes and how to protect against them.

Despite today's highly contentious political climate, the survey results speak to the fact that Americans are aligned on one thing: The majority are concerned about robocall scams in general, especially AI deepfake voice cloning.

The research clearly shows that organizations using omnichannel voter engagement can help increase answer rates with tools like TNS Enterprise Authentication and Spoof Protection and TNS Enterprise Branded Calling to verify and brand outbound traffic.

Upcoming 2025 Report and Predictions

Election season scams are informing the global future of robocall use and abuse. The deepfake strategies the TNS analytics team is seeing in robocall scams during 2024 will have a historic impact on the voice channel for years to come.

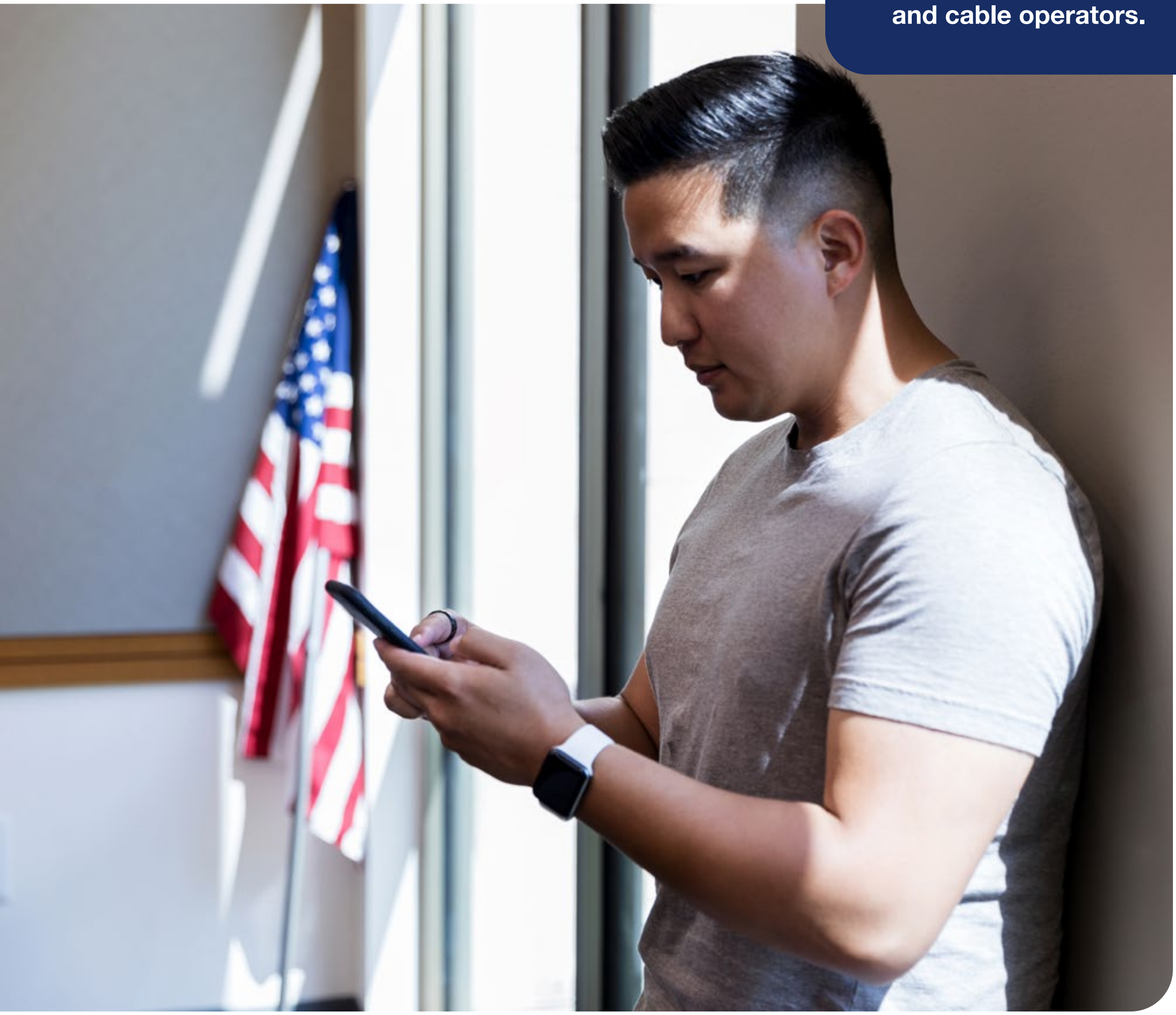
Clever re-directs to data collection websites, with both real and fake URLs, are becoming more common, especially with voice-cloning scams. Though consumers are becoming more wary of bad actors in general, sophisticated deepfakes are providing fresh ways to fool people, steal personal information and misdirect voters.

For all intents and purposes, the top seven carriers are now in full adoption of STIR/SHAKEN protocols – but the majority of VSPs still lag behind in call signing due to budget, resource and SIP interconnectivity issues. Though top carriers are consistently signing close to 90% of calls with the Verstat “A” attestation, the next tier remains stalled at around 25%. Given the overall rising volume of robocalls, this disparity remains a major concern and roadblock to voice-channel parity between operators.

In our upcoming 2025 annual report, TNS will consolidate our 2024 data and take a deeper dive into industry best practices that are proving out against bad actors.

The pressure is on to standardize end-to-end SIP around the world and to enable the network transformation promised by the STIR/SHAKEN security movement. The good news is that more traffic is being identified and labeled for consumers, giving them greater awareness of scams, which callers they can trust and what calls they can answer with confidence, drop or let go to voicemail.

Solutions, including TNS Voice Transit services, provide global call routing via single SIP interconnect technology that enables originated and terminated voice calls between wireless, wireline and cable operators.

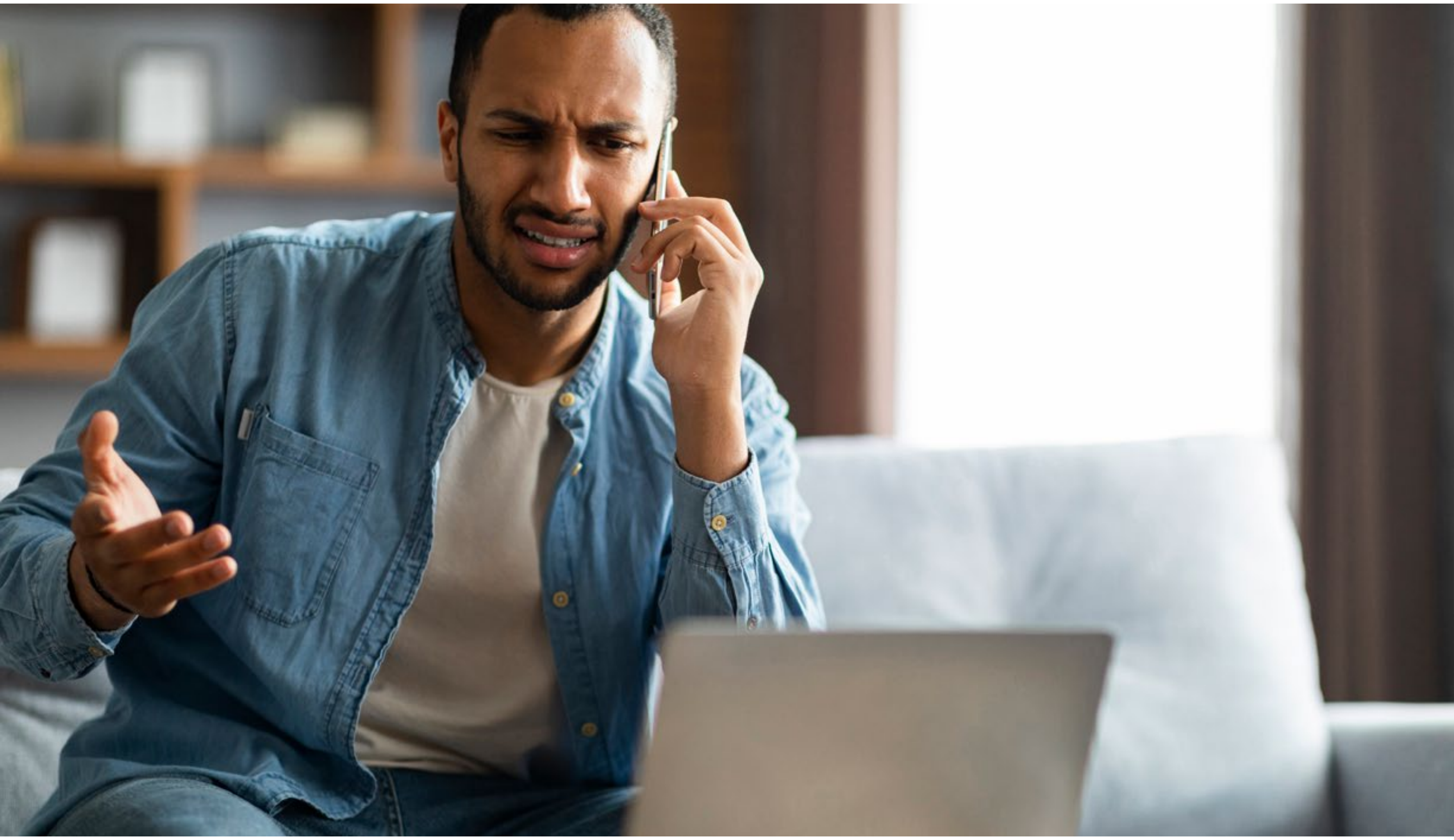


Methodology

TNS analyzes more than 1.5 billion daily call events across hundreds of carrier networks to identify current robocall trends and scams. With TNS' reach extending to almost 250 million active subscribers and unparalleled insights into cross-carrier call events, TNS is uniquely positioned to help carriers differentiate between legitimate robocall activity and scam/nuisance calls. Since TNS reports exclusively on unwanted calls, our data reflects the clearest and most robust infrastructure view across all line types.

1.5 Billion
Daily Call Events

analyzed by TNS across hundreds of carrier networks to identify current robocall trends and scams.



For more information on TNS Call Guardian, Enterprise Branded Calling and Enterprise Authentication and Spoof Protection, contact us at:

tnsi.com/solutions/communications