



**Transaction  
Network Services**

# TNS 2021 1H Robocall Investigation Report

## Seventh Edition

By Transaction Network Services

September 2021



## Executive Summary

3

## Introduction

5

## Primer on Robocalling

6

## Methodology

7

## Results and Analysis

8

## How Carriers Should Address FCC Rule on Automatic Call Blocking

24

## How Can Call Originators Get Customers to Answer the Phone?

26

## Regulatory Updates—2021

29

## Industry Solutions to Combat Robocalling

32

## Conclusions and Recommendations

35



## *The TNS 2021 Robocall Investigation Report, Seventh Edition (Robocall Report)* is a continuing examination into the data, convention and trends that plague consumers' phones daily.

TNS Call Guardian®, the industry-leading big-data analytics engine, has gained insights and reputation data on over 1.7 billion active phone numbers by analyzing 1.3 billion daily call events across hundreds of carriers.

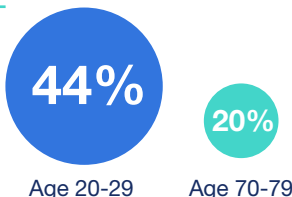
This seventh edition of *TNS' Robocall Report* continues the findings published beginning in 2018 and includes several new insights:

- **Unwanted calls were up in the first six months.** Unwanted calls increased 6% in the first half of 2021 (37.9 billion) compared to the first half of 2020 but were down 10% compared to the same period in 2019. The decline in unwanted calls can be attributed to the COVID-19 pandemic that drove down the volume of unwanted calls in the first half of 2020.
- **Neighbor spoofing using low-volume spamming is a new tactic employed by bad actors.** Use of same area code saw a 127% increase and use of same area code and prefix increased 52% using low-volume spamming techniques across a large amount of telephone numbers in an attempt to avoid analytics engines.
- **VoIP originated calls are the largest portion of unwanted calls.** Sixty-six percent (66%) of all high-risk calls and 61% of all nuisance calls originate from VoIP telephone numbers – representing the largest two sources of these unwanted calls.
- **Wireline is twice as bad as wireless.** While much of the attention is focused on robocalls to mobile phones, 41% of inter-carrier calls placed to wireline numbers in 1H2021 were unwanted, compared to 21% of inter-carrier calls to wireless numbers.
- **Tier-1 carriers continue to be a small part of the problem.** Seventy-five (75%) of the inter-carrier traffic comes from Tier-1 carriers; however, more than 95% of high-risk calls originate from non-Tier-1 telephone resources.
- **STIR/SHAKEN is being adopted by the Tier-1 carriers.** Of the Tier-1 carriers that have deployed STIR/SHAKEN (Secure Telephone Identity Revisited) / (Signature-based Handling of Asserted information using toKENs), more than 50% of the total calls in June were signed, up from 35% in the beginning of the year.

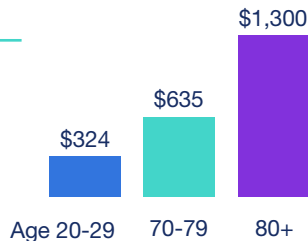
Industrywide:

- Consumers lost more than \$3.3 billion to fraud in 2020—an increase of nearly \$1.5 billion over 2019.<sup>1</sup>
- Imposter scams topped the list of consumer complaints submitted in 2020 to the Federal Trade Commission's (FTC) nationwide Consumer Sentinel; debt scam reductions were second on the list followed by medical and prescription scams as the third highest complaint. These top three scams account for 27% of the complaints to the FTC.<sup>2</sup>
- The FTC saw a 36% increase in complaints received when comparing January-March of 2021 to the same period in 2020.<sup>3</sup>
- Younger people reported losing money to fraud more often than older people. In 2020, 44% of people in their 20s reported a loss to fraud, while only 20% of people in their 70s.<sup>4</sup>
- However, when people in their 70s did lose money, the amount tended to be higher: their median loss was \$1,300, compared to \$324 for people in their 20s.<sup>5</sup>

Younger people  
reported losing  
money to fraud  
more often than  
older people



But when people  
aged 70+ had a loss  
the median loss  
was much higher



<sup>1</sup><https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2020>

<sup>2</sup><https://public.tableau.com/profile/federal.trade.commission#v/home/DoNotCallComplaints/Maps>

<sup>3</sup><https://public.tableau.com/profile/federal.trade.commission#v/home/DoNotCallComplaints/Maps>

<sup>4</sup><https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2020>

<sup>5</sup><https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2020>

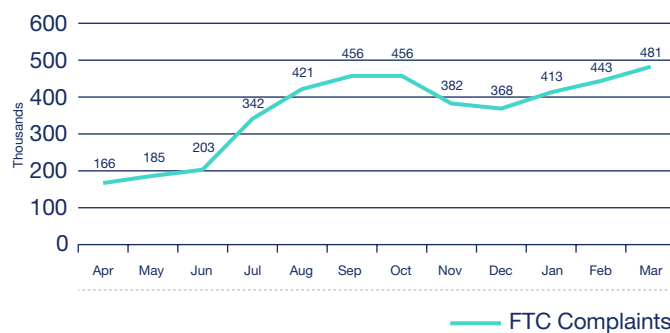


## Fraud amounts to about \$3.3 billion annually



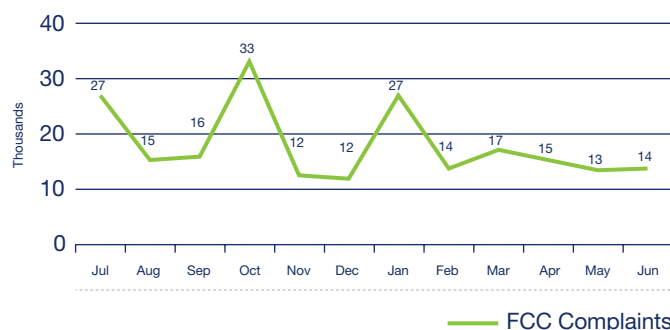
Fraud has become easier for criminals as technology, such as VoIP calling, has enabled both spoofing numbers and low cost robodialing. A 2020 TNS study found that wireless consumers receive roughly 10 calls per week that are unknown. Only 11% of the time will consumers answer an unknown call.

### FTC Do-Not-Call List Complaints—Last 12 Months



- The FCC saw a similar increase in complaints to the Do-Not-Call List, up 55% when comparing January-June of 2021 to the same period in 2020.<sup>6</sup>

### FCC Complaints—Last 12 Months



- More carriers are blocking some of these calls. Carriers also have made low-cost tools available to their wireless subscribers and have educated them on robocalling.

<sup>6</sup><https://opendata.fcc.gov/Consumer/Consumer-Complaints-Data-Unwanted-Calls/vakf-fz8e/data>

### Imposter Scams



About  
**1 in 5 People**  
Lost Money

**\$1,190 Million** Reported Lost  
**\$850** Median Loss

### Identity Theft Reports

**2920%** **Government Benefits Applied For/Received**

**4%** **Evading the Law**

Federal Trade Commission • ftc.gov/data

TNS estimates that nearly 80 billion unwanted calls were placed in the last 12 months.

## Nearly 80 billion unwanted calls were placed in the last 12 months

*The TNS 2021 Robocall Investigation Report, Seventh Edition* is a continuing examination into the trends published in the 2018, 2019 and 2020 Robocall Reports. TNS Call Guardian, the industry-leading big-data analytics engine, has gained insights and reputation metrics on over 1.9 billion phone numbers by analyzing over one billion daily call events across hundreds of carriers.

In addition, this report leverages consumer feedback provided by users of carrier deployed **Enhanced Caller ID** services powered by TNS, shipped to over 250 million mobile devices across more than 550 makes and models.

Billions of data points weave together the robocall stories and statistics from across the country. TNS has expanded this report examining trends on where calls are *terminating* rather than just originating.

In addition, the report takes a closer look at the impact of **donation scams**.

What valuable insights can your organization learn?

## Introduction

*The TNS 2021 Robocall Investigation Report, Seventh Edition* includes a vast amount of factual evidence derived from real network traffic over the last three years.

The study is unique in that it offers an objective, first-hand view of robocalling, spamming and spoofing from the hundreds of carriers that signal across the TNS infrastructure.

Since 1990, TNS has managed some of the largest real-time data communication networks in the world, enabling industry participants to simply, securely and reliably interact and transact with other businesses. TNS provides managed and secure communication platforms allowing enterprises to access the data and applications they need.

TNS leads the development of solutions to help carriers navigate a host of infrastructure complexities and maximize their network reach through the creation of unique multi-service hub solutions.

In this report, TNS presents its interpretation of robocall trends and hopes that both organizations and consumers can benefit from these findings.



The Telephone Consumer Protection Act (TCPA) was passed by Congress in 1991 to regulate the use of automatic telephone dialing systems (auto-dialers) and pre-recorded voice messages.

The specifics of the regulation and the courts’ interpretation are complex and sometimes difficult to decipher but the essence of the law is to safeguard consumer privacy by mandating robocallers obtain explicit consent before placing any ‘non-emergency’ robocall to a consumer’s cell phone, or to landline phones that have been registered on the Do-Not-Call list.

Robocalls are calls made with an auto-dialer or contain a message made with a pre-recorded or artificial voice.

Robocalls are often associated with political and telemarketing campaigns but can also be used for public-service or emergency announcements. Some robocalls use personalized audio messages to simulate an actual personal phone call.<sup>7</sup>

Robocalls are popular with many vertical markets, such as real estate, healthcare, telemarketing and direct sales companies. Many companies who use robocalling are legitimate businesses, but some are not.

When the call is answered, the auto-dialer either connects the call to a person or plays a pre-recorded message. Both are considered robocalls.

Those illegitimate businesses may not just be annoying consumers, they also may be trying to defraud them.

Many robocalls are not wanted and several methods have been developed to prevent unwanted robocalls. The US developed the **Do-Not-Call Registry** in 2003 and allows consumers to opt-out of receiving telemarketing calls on their landline and mobile phones, regardless of whether they are robocalls or not.

As of September 30, 2020, the registry had over 241 million active registrations, an increase of two million registrations from 2019.<sup>8</sup>

However, the lists have been ineffective. While legitimate call originators honor the list, bad actors ignore it. Consequently, a market has developed for products that allow consumers to block robocalls.

Most products use methods like those used to mitigate SPIT (spam over internet telephony) and can be broadly categorized by the primary method used. However, due to the complexity of the problem, no single method is sufficiently reliable.<sup>9</sup>



By creating an industry-leading big-data analytics engine, TNS Call Guardian has maintained a strong focus on aiding calling providers as they seek to restore trust in voice calls.

Call Guardian analyzes over one billion daily call events across hundreds of carriers and creates robocall scoring and categorization on this vast data pool.

More importantly, Call Guardian evolves in response to emerging bad actor trends, such as neighbor spoofing. It perceives the evolution of bad actor calling tactics as a response to measuring and collecting current methodologies.

For example, *Neighbor Spoofing* and *Snowshoe Spamming* occur when the information on the receiver’s phone matches or closely matches the area code and digits like one’s own phone number.

TNS provides extraordinary intelligence because of its deep network integration into carrier networks combined with real-time analytics. This layered approach provides profound insight beyond honey traps and blacklists.

This strategy allows TNS to create accurate and comprehensive reputation profiles differentiating legitimate users from abusive, fraudulent and unlawful ones.

In this way, Call Guardian functions like a trusted credit reporting service continuously collecting reputation data from multiple sources. The system relies on a mix of historical data and real-time intelligence – making use of known legitimate and malicious behavior to train a machine learning algorithm in order to project reputations on virtually any telephone number (TN).

Call management and caller ID applications are designed to protect legitimate phone users (end-users) from illegal robocalls and phone calling scams form a major application area for the service.

These applications are an important source of crowd-sourced reputation data and provide insights that helps identify callers who may be violating state and federal laws, most notably scammers who use robocalls in a criminal enterprise like identity theft or fraud.

The dynamic nature of the service means that non-binary reputation “scores” along with other helpful insights are supplied on a query-answer basis. Instead of lists, the service supports queries to APIs (application protocol interface) to ensure the most accurate reputation score is available in real-time.

TNS provides Enhanced Caller ID that is used by most of the leading US wireless service providers as well as Call Guardian to US landline providers.

Layered Approach to Identifying Bad Actors

	DNC List, FCC Complaint Data
	DNO, Invalid, Unassigned, Unallocated Telephone Numbers
	INP Data, NPAC Data, LERG Data, Toll-Free Routing Data
	VoLTE / VoIP Peering
	Crowd-Source Data, Honeypot Data
	Enterprise Data
	STIR/SHAKEN Parameters
	Fraud, Spam and Premium Rate Called Numbers
	Machine Learning Algorithm—Real-Time Scoring of 1.9B TNs

<sup>7</sup><https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts>  
<sup>8</sup><https://www.ftc.gov/news-events/press-releases/2019/10/ftc-releases-fy-2019-national-do-not-call-registry-data-book>  
<sup>9</sup><https://ieeexplore.ieee.org/document/7548510/>







## Reputation Category and Scoring

TNS uses reputation categories to score common call behavior. This reputation scoring provides insight as to the certainty of this categorization and severity of consequences.

Categories are indicative of legitimate, abusive, fraudulent and unlawful call behavior—inclusive of any call placed via auto-dialer or manually dialed.

Each carrier can choose what category to display on the device, for example “Potential Spam.”

TNS offers a dispute resolution process for call originators to challenge reputational categories assigned to its telephone numbers.



### Positive Robocalls

Present no harm to subscribers; some of these robocalls may even be wanted/needed.

Examples Include:

**Public service announcement**

Calls that are placed to inform a community of an event, such as a school closing.

**Appointment confirmation**

Calls made to confirm an appointment with a customer from a utility, service provider or doctor's office.

**Prescription refills**

Calls made to remind a consumer that a prescription needs to be refilled by a pharmacy.

### Nuisance Robocalls

The severity of harm of a nuisance call is moderate. The calling behavior isn't indicative of malicious intent or negligent non-compliance. These involve harm caused by careless, not intentional calling patterns.

Examples Include:

**Promotional offers**

Calls made to customers who have not given prior explicit consent.

**Solicitation**

Calls made for charitable purposes to customers who have not given prior explicit consent.

**Accounts receivable**

Calls made multiple times per day for the collection of a delinquent debt or other financial matters that become harassing to the subscriber.

### High-Risk Robocalls

High-risk calls typically cause emotional distress while the severity of harm often includes loss of money, invasion of privacy and identity theft, all hallmarks of a major crime.

Examples Include:

**Social security scam**

Calls that tell you your social security number has been suspended.

**COVID-19 cures**

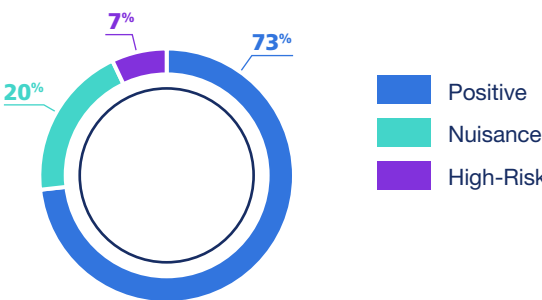
Calls selling fraudulent products that claim to prevent mitigate or detect the coronavirus.

**Credit card interest scams**

Calls telling you that you are eligible to receive a reduced interest rate intended to get your personal information.

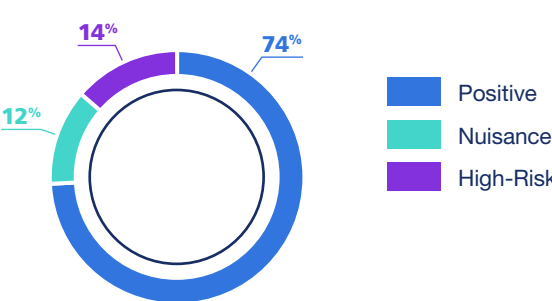
TNS found that 27% of the inter-carrier calls in 1H2021 were scored as unwanted, consistent with 2020. Unwanted represents non-positive calls or those that are scored as nuisance or high-risk.

Scoring by Category—1H2021



The first half of 2021 has shown a noticeable shift in the mix of unwanted calls with nuisance calls making up a much larger portion. Nuisance calls were 12% in 2020 compared to 20% in first half of 2021.

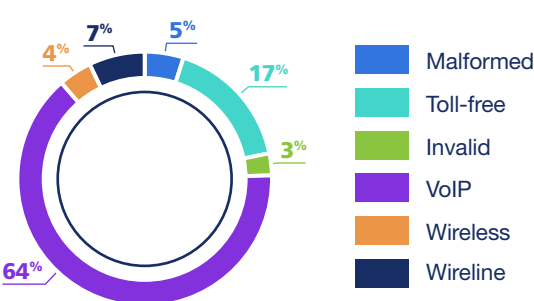
Scoring by Category—2020



### Origination of Unwanted Calls

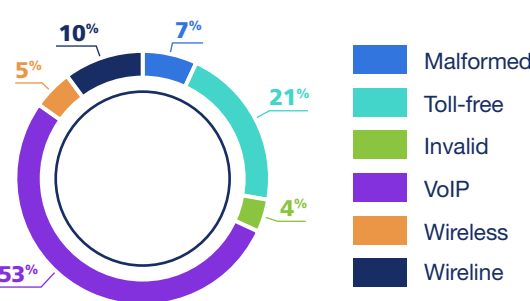
VoIP-originated calls accounted for 64% of the unwanted calls in 1H2021 by total volume, up significantly from 53% in 2020. Toll-free calls were the second highest at 17%.

Distribution of All Unwanted Calls—1H2021



**VoIP calls grow to be larger part of the high-risk calls**

Distribution of All Unwanted Calls—2020



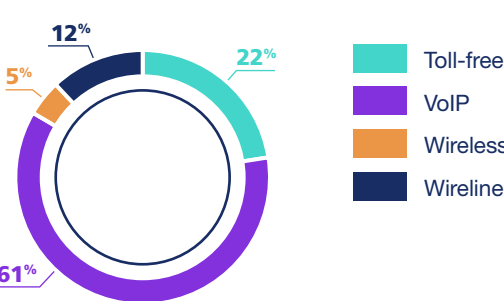
A provider that allows users to bring their own device and unbundles service so that direct inbound numbers may be purchased separately from outbound calling minutes are another source for bad actors.

A carrier that doesn't follow established hardware standards (such as Skype) or locks subscribers out of configuration settings on hardware that the subscriber owns outright (such as Vonage) is more restrictive.

Providers that market “wholesale VoIP” allow any displayed number to be sent, as resellers will want their customer's numbers to appear.<sup>10</sup>

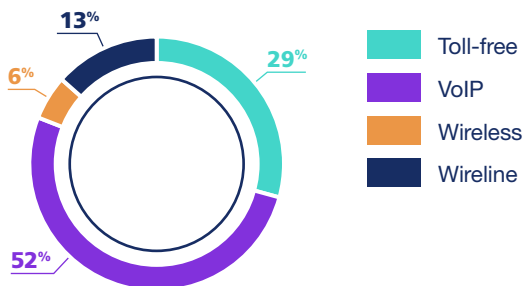
Nuisance calls continue to be led by VoIP telephone numbers and the share of nuisance calls coming from VoIP telephone numbers increased from 52% of the calls in 2020 to 61% of the calls for in 1H2021.

Distribution of Nuisance Calls—1H2021



<sup>10</sup><https://www.fcc.gov/document/fcc-urges-more-phone-industry-join-tracing-scam-robocalls>

### Distribution of Nuisance Calls—2020

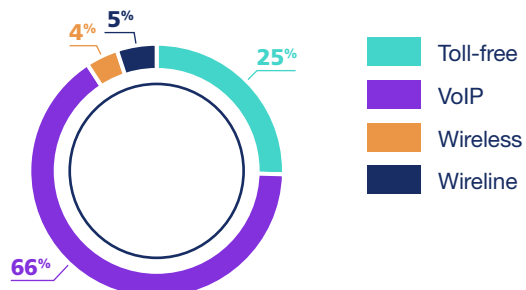


While there are legitimate reasons to modify the calling number, bad actors use this technique to hide their identity.

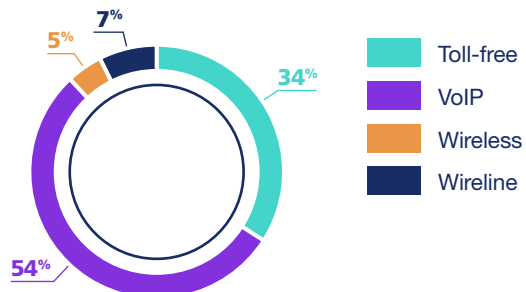
A malformed telephone number does not have 11 digits or does not start with 1. An invalid telephone number is well-formed but is not in a valid LERG block (NPA-NXX) and not in a valid toll-free area code.

VoIP telephone numbers still represent the largest source (66%) of high-risk calls, in 1H2021, up significantly from 54% in 2020. Invalid and malformed numbers are in the “Other” category along with toll-free numbers and are the second highest source of high-risk calls in the charts below.

### Distribution of High-Risk Calls—1H2021



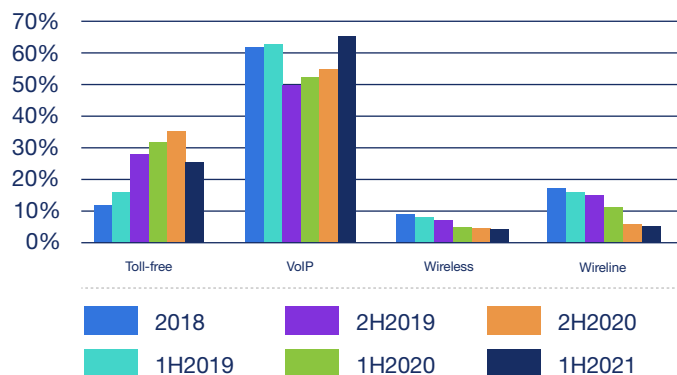
### Distribution of High-Risk Calls—2020



Spoofing of wireless telephone numbers declined from 2020 to 1H2021. They have shifted to near-neighbor spoofing where the area codes are the same, but not the first five or six digits which is being done primarily by VoIP numbers.

Bad actors appear to have shifted from originating calls utilizing toll-free numbers to VoIP telephone numbers. Unwanted, high-risk calls from VoIP telephone numbers jumped to 66% in 1H2021 from 55% in 2H2020, as you can see from the chart below. Toll-free numbers, however, continue to rank as second highest.

### Distribution of High-Risk Calls Over Time



High-risk calls shifted from toll-free to VoIP and Neighbor Spoofing

The extension of the **STIR/SHAKEN** deadline for small service providers that have under **100,000 subscribers** has likely resulted in the increase of unwanted VoIP calls.

The FCC proposed to shorten by one year the extension for small voice service providers that originate an especially large number of calls. Those providers must implement STIR/SHAKEN in the IP portions of their networks no later than June 30, 2022. They believe this proposal will protect Americans from illegal robocalls by ensuring that call providers, most likely to be the source of robocalls, authenticate calls sooner.<sup>11</sup>

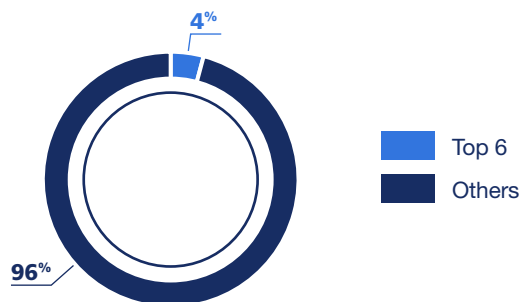
One of the reasons cited for the basis of action in the *Notice of Proposed Rulemaking* is data from the *TNS 2021 Robocall Investigation Report, Sixth Edition*, that was released in March 2021.

<sup>11</sup><https://docs.fcc.gov/public/attachments/FCC-21-62A1.pdf>

In a recent filing to the FCC, USTelecom indicated that most Industry Traceback Group (ITG) tracebacks identify smaller, VoIP-based providers as the originator for illegal robocalls whether those calls originate in the US or abroad. Tracebacks seldom conclude that a large provider originated the robocall, or even that a smaller facilities-based provider did such as a rural local exchange carrier (LEC) or rural wireless provider.<sup>12</sup>

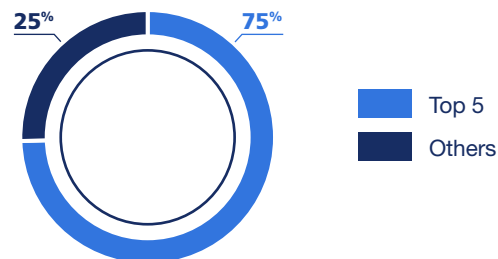
It is important to note that only 4% of the high-risk calls in 1H2021 originated from the top six carriers (AT&T, CenturyLink, Charter, Comcast, T-Mobile and Verizon). This is a significant drop from 11% in 2019 and down from 6% in 2020.

### Telephone Numbers Placing High-Risk Calls



The Tier-1s account for 75% of the total number of calls in 1H2021, up slightly from 67% in 2020. However, the Tier-1s are a declining percentage of high-risk calls.

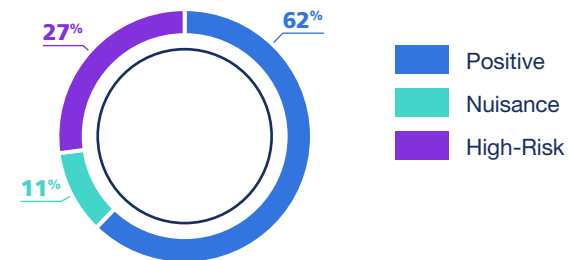
### Telephone Number Resources—Total Calls



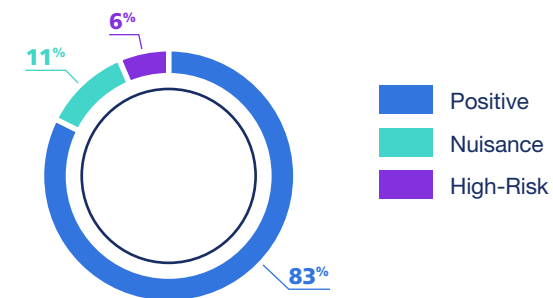
VoIP networks make it relatively easy to spoof caller ID. While most unwanted calls continue to originate from VoIP numbers, the percentage of *unwanted* VoIP calls went up to 38% in 1H2021, more than double from 2020 (17%).

TNS believes this is due to low-volume spammers using VoIP numbers to generate robocalls.

### Scoring of VoIP Telephone Numbers—1H2021



### Scoring of VoIP Telephone Numbers—2020

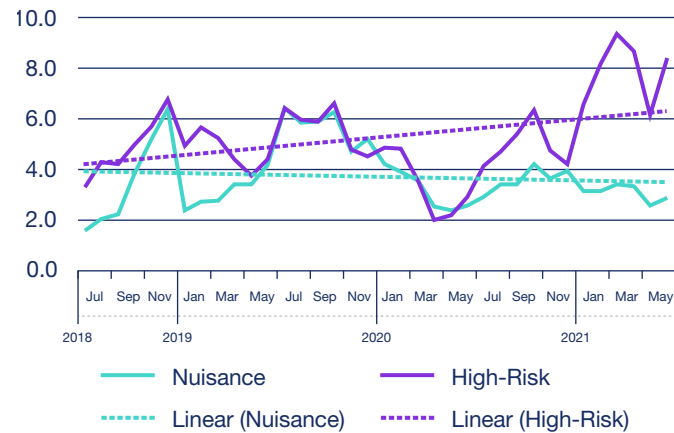


Over 95% of scam/fraud calls come from numbers not owned by Tier-1 carriers

<sup>12</sup><https://go.tnsi.com/us-telecom-comments>

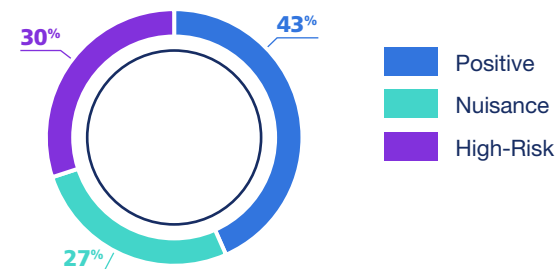
Bad actors are using VoIP originating networks. The number of nuisance calls, on a per subscriber basis, coming from a VoIP number, has stayed relatively flat to slightly declining. However, the number of high-risk calls, per subscriber, has more than doubled, up 123% in comparing 1H2021 to 1H2020.

#### Unwanted Calls per Telephone Number—VoIP

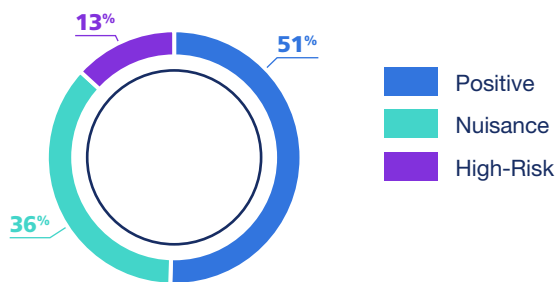


The percentage of unwanted calls coming from toll-free numbers has increased from 49% in 2020 to 57% in 1H2021.

#### Scoring Distribution Toll-Free Calls—1H2021



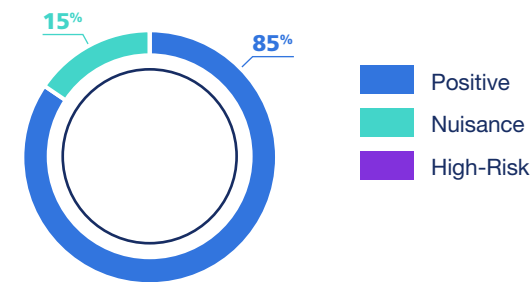
#### Scoring Distribution Toll-Free Calls—2020



## Top 10 toll-free calls have moved to high-risk from nuisance

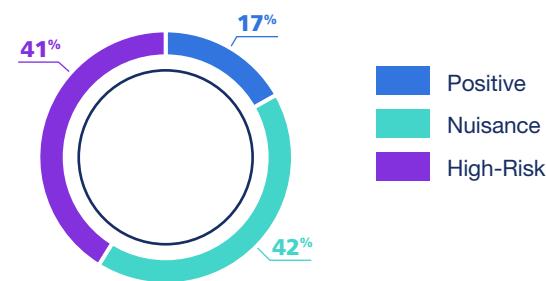
Of the top 10 toll-free numbers in 1H2021 in terms of call volume, 83% of the calls are scored as positive from TNS, up from 71% in 1H2020. This jump is due to an increase in enterprise and government agencies registering toll-free numbers.

#### Scoring of Top 10 Toll-Free Numbers by Volume—1H2021



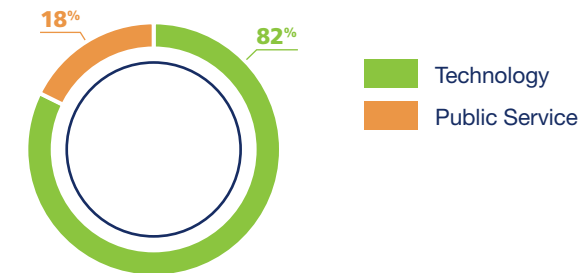
The crowd-sourced data from the top 10 toll-free numbers, however, is overwhelmingly considered nuisance or high-risk by the subscriber.

#### Crowd-Sourced Sentiment of Top 10 Toll-Free Numbers—1H2021



The top ten companies are legitimate call originators and represent large technology companies or provide public services to the community.

#### Category of Top 10 Toll-Free Numbers by Volume—1H2021



The risk of missing an important phone call was heightened during the COVID-19 pandemic last year. One of the biggest challenges contact tracers faced is an unexpected one: robocalls. Scammers are spoofing legitimate government and health agency phone numbers to trick people into surrendering money or personal information, and the public has been conditioned over the past several years to stop answering calls from unknown numbers, leading them to mistrust or not answer legitimate contact tracing efforts. Because of this, wireless carriers, government health agencies and industry leaders are working to authenticate call identification information for consumers and improve answer call rates for legitimate contact tracing calls.

There is a key reason for this phenomenon: consumers have been hammered with a variety of increasingly convincing robocalls in the past few years, including many claiming to be well-known companies like Apple and Amazon. Most, if not all, of Apple's store phone numbers have been spoofed at some point. The calls sound legitimate, provide a secondary "customer service" number to call and immediately begin harassing the victim.

Displaying call information, though a step in the right direction, is still not enough. While an incoming call might display a logo, it doesn't eliminate the possibility that the call could be spoofed by a bad actor. To overcome this issue, carriers must turn to advanced data analytics to parse the massive volumes of daily call events and identify patterns in emerging robocall tactics. This allows carriers to authorize use of a phone number and accompanying call information, thus further improving trust with the consumer. In fact, marking a call as authorized and authenticated increases the likelihood of a consumer answering by as much as 29%.

At a time when the importance of being able to reach Americans by phone has been clearly illustrated through contact tracing efforts, policy, telecom and industry leaders are taking steps to help boost trust in voice calling again. Branding incoming calls has been shown to increase that trust when paired with a reliable analytics component that helps to verify that calls are not being spoofed.

The SHAKEN framework, developed by the ATIS-SIP Forum IP-NNI Task Force, is a call authentication framework designed specifically to mitigate unwanted robocalls by reducing caller ID spoofing. However, the framework was never intended to be a complete solution for the robocalling problem. Rather, SHAKEN is a critical tool that will move the yardsticks.<sup>13</sup>

Third-party call centers are a great example of a situation that will not allow full attestation by SHAKEN today. However, there are several ideas that are being developed to address this issue.

TNS sees this as a potential area a bad actor can exploit in the SHAKEN framework and will continue to work with the industry to remedy this issue.

## Branded calling could help improve crowd sentiment of toll-free numbers

### Termination of Unwanted Calls

Total calls to wireless telephone numbers have now *exceeded* calls to wireline and VoIP telephone numbers. This phenomenon isn't surprising with cord-cutting of home telephone service continuing and more reliance on smartphone devices by younger consumers.

<sup>13</sup>[https://www.atis.org/01\\_strat\\_init/dlt/docs/shaken-faq.pdf](https://www.atis.org/01_strat_init/dlt/docs/shaken-faq.pdf)

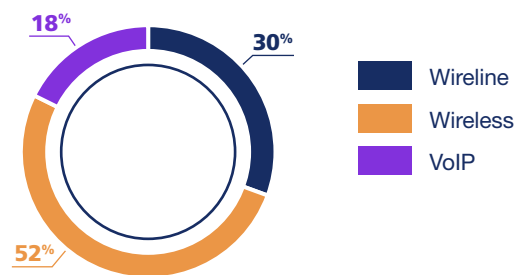


## Calls to wireless telephone numbers now exceed wireline and VoIP combined



Calls to wireless telephone numbers account for 52% of the total call volume for 1H2021, up from 46% in 2020. Wireline call volume has decreased 12% while wireless has increased 7% comparing 1H2021 to 1H2020.

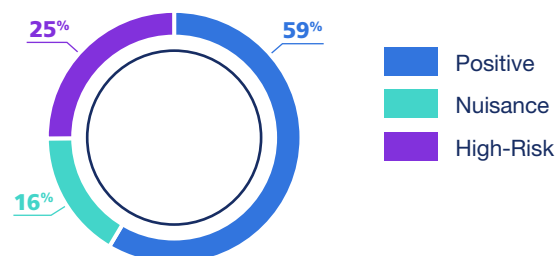
**Total Call Distribution Called Telephone Number—1H2021**



VoIP numbers represent telephone numbers utilized by the cable operators (MSOs) and VoIP providers.

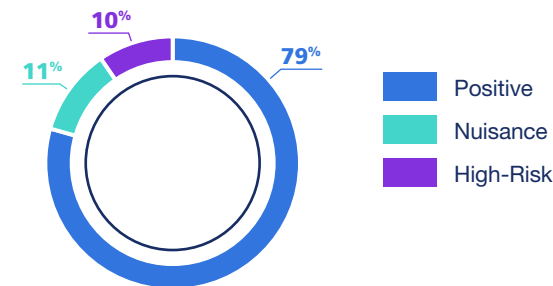
While much of the attention goes towards robocalls to mobile phones, TNS finds that 41% of wireline calls in 1H2021 were unwanted, compared to 21% to wireless numbers.

**Distribution of Scoring for Wireline Telephone Numbers—1H2021**



Unwanted to calls to wireless numbers are only 21% of the total volume with high-risk and nuisance calls split evenly.

**Distribution of Scoring for Wireless Telephone Numbers—1H2021**

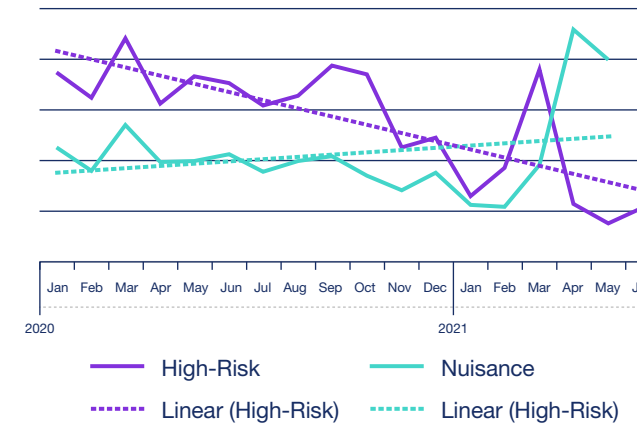


**Wireline twice as likely to receive an unwanted call than wireless**

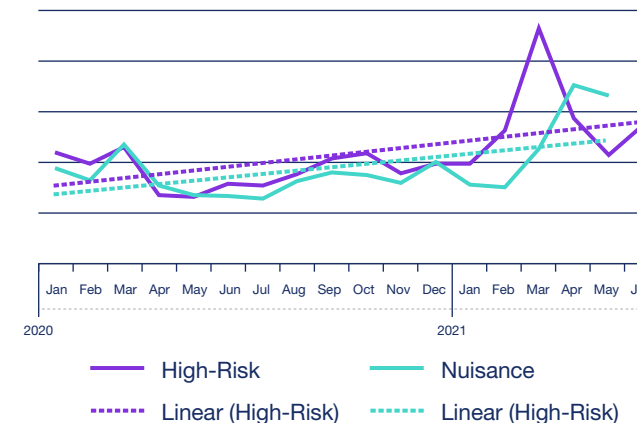
The percentage of unwanted calls to wireline numbers dropped 14% when comparing 1H2021 to 1H2020. This is consistent with the overall decrease in total wireline call volume. However, the percentage of unwanted calls to wireless numbers increased 20% in this same period mostly due to the effects of COVID-19 and a drop in calling volume from April through June.

Both wireline and wireless high-risk calls declined in 2020 but the number of nuisance calls increased. Wireline nuisance calls increased 45% while wireline high-risk calls decreased 54% in 1H2021. At the same time, wireless nuisance calls increased 79% while high-risk calls decreased 33% in the period noted above. Again, the increases are skewed by the lockdown from COVID-19 in 2020.

**Wireline Unwanted Call Trend**



**Wireless Unwanted Call Trend**



TNS recognizes that the difference is in whether these call blocking and labeling services are offered as an opt-out or opt-in basis and could be impacting who bad actors target. In addition, older Americans typically have a home phone line while younger consumers are either a cord-cutter or have never had landline service.



**Opt-in subscriber services may be impacting bad actors**

## Call Blocking Tools Available to Consumers: Second Report on Call Blocking

The Consumer and Governmental Affairs Bureau released a Staff Report on the state of deployment of advanced methods and tools to eliminate illegal and unwanted calls. This section tries to highlight the efforts made by AT&T, Bandwidth, Charter, Comcast, Cox, Frontier, Lumen, TDS Telecom, T-Mobile, USCellular, Verizon and Vonage all of which offer free blocking services, often through a third-party analytics company.<sup>14</sup>

The major *wireless* providers offer call blocking and labeling services on an opt-out basis.

- AT&T Wireless offers *Call Protect* for free
- T-Mobile offers *Caller Screener* for free for Android users and *Scam Shield* for post-paid users
- Verizon Wireless offers *Call Filter* for free and in September 2020, Verizon and Apple, partnering with TNS, provided a new *Silence Junk Callers* feature to Verizon Call Filter customers using iPhones. The feature is enabled by *default* to forward to voicemail all high and medium-risk spam calls

However, the major *wireline* providers offer call blocking and labeling services on an *opt-in* basis.

- AT&T offers *Digital Phone Call Protect* for free
- Lumen offers VoIP customers a free blocking service
- Comcast offers their VoIP residential subscribers a free blocking service
- Verizon offers two free solutions, *Spam Alerts* as an opt-out service and a call-blocking service for VoIP residential customers that is opt-in



<sup>14</sup><https://docs.fcc.gov/public/attachments/DA-21-772A1.pdf>





AT&T has a network-based, provider-initiated, call blocking program run by the AT&T Global Fraud Management Organization that blocks suspected illegal calls on its network and terminating to AT&T and non-AT&T customers by relying on network intelligence and a team of fraud investigators.

Bandwidth states that it operates a network that is entirely optimized for IP-technology and is predominately an underlying service provider to other IP-based communications companies. Bandwidth has added STIR/SHAKEN feature functionality, such as enabling intermediate transit identity header and in-bound identity header delivery.

Charter automatically blocks, at the network level, calls that appear to originate from numbers on the DNO list. Charter offers Call Guard, an advanced caller ID and robocall-blocking solution, at no charge to Spectrum Voice and Spectrum Business Voice customers, on an opt-out basis; TNS Call Guardian is the underlying technology for Call Guard and uses industry-leading data, STIR/SHAKEN.

Comcast has a new caller ID verification tool for all residential as well as small and medium-sized business customers. This tool provides more information about the level of trust associated with a particular call by displaying the word “Verified” (or the letter “V”) any time the caller’s provider has confirmed that the call is coming from a legitimate telephone number.

Cox provides network-based call blocking (Edge Blocking) for DNO, invalid and unallocated telephone numbers. The primary call blocking tool, Nomorobo, is a third-party service, which automatically identifies and blocks potential unwanted and illegal calls using Simultaneous Ring technology.

Frontier explains that it has deployed STIR/SHAKEN on its IP network and has begun exchanging authenticated STIR/SHAKEN traffic. Frontier conducts network-level call blocking for numbers on the DNO list. Frontier also offers several opt-in call blocking tools across both its IP and TDM networks, free of charge, including anonymous call rejection, selective call rejection and selective call acceptance.

Lumen monitors its networks for mass calling events and coordinates with other major providers, the ITG, trusted third parties, and key federal agencies to address and mitigate obvious fraudulent calls at the network level. In coordination with the ITG, Lumen performs DNO blocking of government impersonation.

TDS Telecom uses TNS Call Guardian Authentication Hub to provide a network-level tool to identify robocalls. This network-level tool works on the IP and TDM portions of the network to maximize call blocking.

T-Mobile provides Scam Block in addition to Scam Shield, which blocks calls identified as “Scam Likely” at the network level. Number change provides a new number for customers who have become spam targets, while T-Mobile PROXY provides a second number for some customers. T-Mobile customers can control the call blocking features through the free Scam Shield application, which also offers the option of premium services like the ability to send entire categories of unwanted calls to voicemail, create “always block” lists, and set up voicemail-to-text services. These additional features are included for T-Mobile customers with Magenta MAX plans; regular subscribers pay \$4.00 per month per line.

USCellular offers call blocking through TNS Call Guardian. Call Guardian provides customers with the ability to know they are receiving a potentially fraudulent call and the capability to block the call at their device. USCellular’s VoLTE-enabled subscriber base has free network-level call analytics tools and blocking. In addition, Call Guardian is being used by approximately 9% of USCellular subscribers.

Verizon, at the network level, has blocked hundreds of millions of calls across-the-board where the calling party number is invalid or unassigned, or where the person to whom the number was assigned has authorized the block. Verizon works vigorously with the ITG and passed to the ITG numerous leads about illegal COVID-19 scams based on calls to numbers identified by its honeypot (i.e., a decoy to lure attacks), so that law enforcement could take appropriate action.

Vonage offers its Spam Shield service to business customers, which identifies suspected spam within the caller ID to allow the called party to decline the call; since August 2020, Vonage offers an equivalent service to residential customers.

In addition, the FCC has also been aggressively enforcing action against illegal robocallers including against gateway providers that facilitated COVID-19-related scam robocalls.<sup>15</sup>

Top Scams

There are different tactics that criminals use to defraud millions of people. They use robocalls to convince consumers to give out their personal information or send money.

In a bid to help consumers avoid these scams, TNS catalogs the top scams and publishes them on its website.

**Donation scam**—These scams pose as a legitimate charity, make up a fake organization name that sounds trustworthy or even create a registered charity but misuse funding. Unfortunately, using the words “police” or “firefighters” in a charity’s name does not confirm any of the money raised is benefiting these groups or that police and firefighters are even a part of them.

**Auto warranty scam**—This scam involves posing as representatives of a car dealer, manufacturer or insurer telling you that your auto warranty or insurance is about to expire. The call will include some sort of pitch for renewing your auto warranty or policy.

**Debt collection scam**—These scams take on many forms. Typically, the bad actor spoofs a legitimate toll-free number of a legitimate credit card company and asks for your sensitive personal information. You should never provide anyone with this information unless you are sure they’re legitimate. Validating this is as simple as asking the caller for a name, company, street address, telephone number and professional license number.

**Home buying scam**—The scams begin by asking what kind of property you own and if you are interested in selling it, attempting to make the call sound legitimate. Then they will make a bogus offer, possibly one you cannot refuse. The catch—there is an “administrative fee” which, after being paid, results in the bad actor riding off into the sunset. Legitimate buyers would not ask for a fee to paid on the initial offer, so if this happens, hang up immediately.

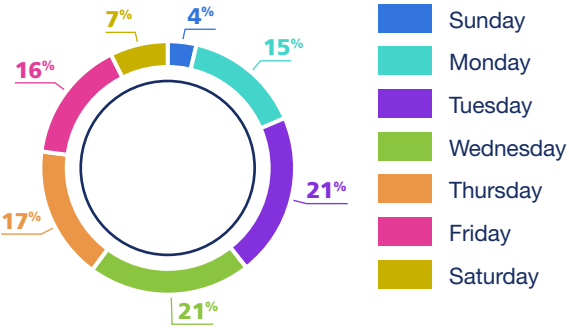
**Political scam**—These scams take on three forms:

- 1. **Cash Donations**—Scammers impersonate or spoof legitimate political campaigns to gain your credit card information.
- 2. **Surveys and Prizes**—Scammers pretend they will give you a prize after completing a survey and ask for your credit card number after the survey.

The number of unwanted calls varies daily but the highest volume of unwanted calls was on Tuesday during 1H2021 (21%). The weekend represented 11% of the total volume of calls, a slight decrease from 14% in 2020.



Day of Week for Unwanted Calls—1H2021



Donation scam had highest volume on heaviest day in 1H2021

The day with the highest volume of unwanted calling occurred on June 17, 2021 involving a donation scam. Donations are a great way to support causes you hold close to your heart, but scammers are notoriously good at tricking those who are passionate about an issue and want to help through funding, so it is important to be very cautious when making donations.

Some legitimate non-profit organizations have confirmed they do not solicit donations over the phone. For example, the National Police Foundation does not solicit donations from anyone via phone, according to its website. There is no safe way to confirm the identity of the caller, so never give your credit card, address or other personal information over the phone.

The Federal Trade Commission (FTC) has received 2,095 fraud incident reports for charitable contributions totaling \$2.8 million in the first quarter of 2021.<sup>16</sup>

<sup>15</sup><https://www.fcc.gov/document/call-blocking-report-tools-now-substantially-available-consumers>

<sup>16</sup><https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts>



## FTC Consumer Sentinel Network

Charitable Solicitations Year: 2021 YTD

### Fraud Facts at a Glance

# of Fraud Reports: **2,095**

% Reporting \$ Loss: **25%**

Total Loss Reported: **\$2.8M**

Median Loss Reported: **\$450**

Top Payment Method: **Gift Card or Reload Card**

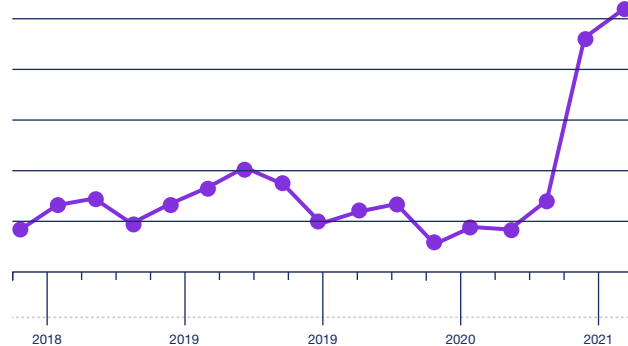
Top Contact Method: **Social Media**

State rankings are based on the number of reports per million population.  
The District of Columbia and Puerto Rico are not included in ranking.

Federal Trade Commission • ftc.gov/data

The total number of reports and dollar loss submitted to the FTC has grown dramatically in 2021.<sup>17</sup>

### Fraud Reports by # of Reports Charitable Solicitations



The FTC provides important questions to ask a caller regarding the charity including:<sup>18</sup>

- What is the charity's exact name, web address and mailing address?
- How much of my donation will go directly to the program I want to help?
- Are you raising money for a charity or a Political Action Committee (PAC)?
- Will my donation be tax-deductible?

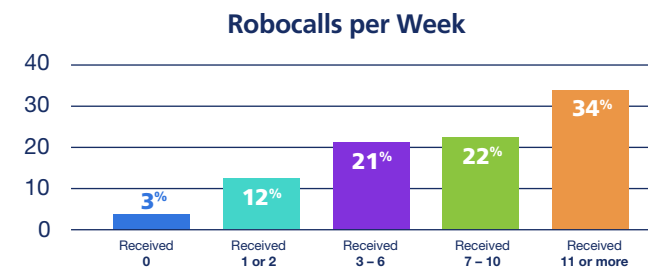
In addition, the callers must follow certain rules:<sup>19</sup>

- They can't call you before 8 am or after 9 pm
- They must tell you the name of the charity and tell you if the reason they're calling is to seek a donation
- They can't deceive you or lie about:
  - The fundraiser's connection to the charity
  - The mission or purpose of the charity
  - Whether a donation is tax-deductible
  - How a donation will be used, or how much of the donation actually goes to the charity's programs
  - The charity's affiliation with the government
- They can't use a robocall or pre-recorded message to reach you unless you are a member of the charity or a prior donor—and even then, they must offer you a way to opt-out of future calls.
- The caller ID on your phone has to show the name of the charity or fundraiser, along with a number that you can call to ask to be placed on the charity's do-not-call list.

A TNS survey in 1H2020 found that 53% of US *senior citizens* believe robocallers tried to scam them out of personal information in 2019; and nearly as many (47%) reported that they were targets of financial scams in 2018.<sup>20</sup>

Additional findings from the survey are the following:

- **Robocall volume is high among seniors.** Eighty-nine percent (89%) of seniors receive at least one robocall per week while more than half (56%) receive at least seven robocalls per week.
- **Seniors in dark about healthcare scams.** Even though 45% of seniors received a healthcare-related scam call, only 21% reported that they received information from their healthcare provider on robocall scams; this is problematic as older Americans are vulnerable to health scams fueled by the pandemic.
- **Seniors lack awareness of robocall filtering apps.** While 25% of respondents use a robocall blocking app from their carrier, two-thirds (66%) of seniors are not aware if their carrier offers such protection—suggesting an opportunity for carriers to broaden app branding and education efforts.



TNS conducted another survey earlier this year to understand the *consumer frustration* with robocalls.

- **Pandemic highlights need for Branded Calling.** Health agencies have struggled to reach Americans via phone with important COVID-19 vaccine and exposure information. Why? Seventy-seven percent (77%) of consumers never answer phone calls from numbers they do not recognize, highlighting the need for carriers to offer accurate branded calling, or enhanced Caller ID. Sixty-three percent (63%) of respondents would answer a call if the logo of a brand they recognized was displayed.
- **Consumers are confused about robocall blocking and reporting options.** The good news is that 38% of consumers have a robocall blocking app through their carrier and 19% use an over-the-top app. Now the bad news: more than half (51%) of consumers do not even know if they have a robocall blocking app on their smartphone - pointing to a need for more market education that free tools are available through the carrier. At the same time, only 28% of respondents submitted a robocall complaint to their state Attorney General, the FTC or the Do-Not-Call Registry.
- **Millennials are most fed up with robocalls.** Millennials consistently outpaced other "generations" when it came to robocall frustration.


- **Robocalls to wireline home phones overlooked.** Overall, 78% of respondents, and 90% of 55-64-year-olds, believe robocalls to wireline phones are a growing but are an overlooked problem. And given that 57% of consumers said most calls to their home phone (if they have one) are robocalls, it is hardly a surprise that nearly three in 10 (29%) got rid of their wireline phone service because of robocalls.
- **Americans want robocall scammers to pay...with jail time.** Eighty-five percent (85%) believe robocallers who try to scam consumers should get jail time while 90% believe these robocalls should pay a financial penalty/fine. When asked who was responsible for stopping these calls, answers were mixed: federal government (20%); my wireless/wireline carrier (18%); businesses trying to sell me the products/services (9%); robocall blocking mobile app vendors (6%); my state government (5%); 35% said all the above are responsible.


## TNS 2021 Robocall Report: Americans Deluged with 80 Billion Unwanted Calls Over Past Year

TNS' bi-annual report finds that Tier-1 US carriers account for less than 5% of high-risk calls, affirming a continued shift in robocall activity to smaller carriers and VoIP providers.

### Scammers Become More Sophisticated; Change Robocall Methods and Tactics


#### Scammers Shift to VoIP Networks


 With Tier-1 high-risk call volume down, robocallers are turning to VoIP networks, which account for the largest share of unwanted calls.

 66% of all high-risk calls and 61% of all nuisance calls originate from VoIP telephone numbers – two of the highest sources of spam.

 The percentage of unwanted calls on VoIP networks increased to 38% in the first half of 2021, rising from 23% in the first half of 2020.

#### Robocallers Double Down on Home Wireline Phones

 While much of the robocall attention centers around mobile phones, 41% of calls placed to wireline numbers in the first half of 2021 were unwanted compared to 21% of calls to wireless numbers.

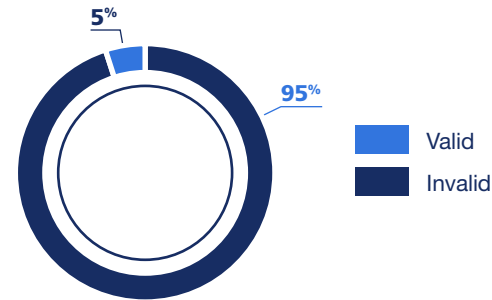
 Because wireline numbers are now twice as likely to receive unwanted calls as wireless numbers is a reminder that robocalls aren't just a mobile phone problem.



### Invalid/Unallocated Number Use

The one constant in the robocall dilemma is that bad actors change tactics quickly. Using spoofed numbers is one of those tactics. Spoofing of invalid/unallocated numbers increased an incredible 150% comparing 1H2021 to 1H2020. However, it is important to note that invalid/unallocated numbers remain a small percentage of total unwanted call volume at just 5%.

Unwanted Calls by Valid/Invalid NPA-NXX



In November 2017, the FCC adopted rules allowing providers to block calls from numbers on a Do-Not-Originate (DNO) list and those that come from invalid, unallocated or unused numbers.

The FCC issued a Declaratory Ruling in June 2019 that expanded the ability of voice providers to block certain categories of robocalls. In this far-reaching ruling, the FCC specifically authorized – but did not require – voice providers to offer consumers programs that block unwanted calls using reasonable analytics (“call blocking programs”) on an opt-out basis.

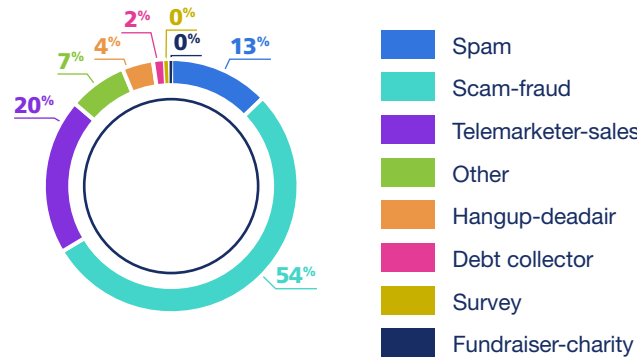
### Crowd-Sourced Statistics

As part of its Identity and Protection portfolio, TNS provides **Enhanced Caller ID** that is used by most leading US wireless service providers, as well as **Call Guardian** to US landline and cable providers.

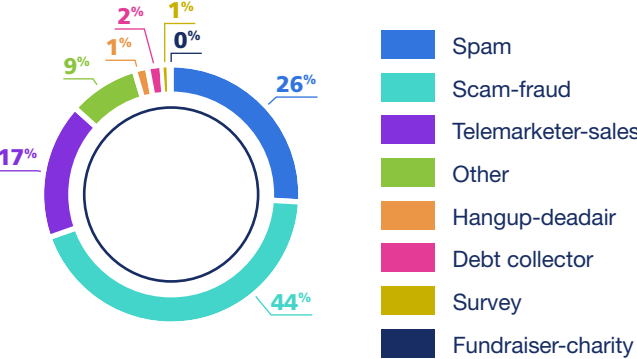
Enhanced Caller ID identifies callers or texters with their names displayed directly in the incoming call screen and message threads, even if their number is not in contacts.

The end-users of TNS services provide direct feedback through the mobile device and have classified robocalls in the following categories: 67% are classified as spam or scam-fraud, and 20% are marked as telemarketing-sales. The scam-fraud and telemarketing-sales category has increased while spam category decreased.

Crowd-Sourced Feedback by Major Category—1H2021



Crowd-Sourced Feedback by Major Category—2020



When the end-users leave comments associated with unwanted calls, the top words used are:

1. Scam/scammer
2. Spam
3. Warranty/car insurance
4. Social security
5. Amazon



### Neighbor Spoofing

Bad actors have used spoofing as a tactic to trick consumers into answering their spam calls. The information on the receiver’s phone matches or closely matches the area code and several digits like one’s own phone number – which makes the consumer more likely to trust the call and answer.

To combat this, TNS launched its **Neighbor Spoofing** feature in mid-2018 and has continued to evolve it to protect consumers.

TNS’ Neighbor Spoofing analyzes, detects and establishes a reputation for phone numbers and phone calls to help consumers evaluate if a call with a familiar area code is legitimate.

A combination of deep carrier network integration along with real-time intelligence of Call Guardian is how TNS is leading in combating this tactic.

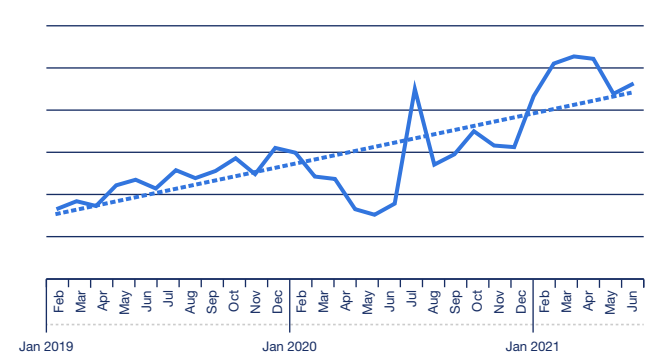
TNS has observed an increase in bad actors that are using low-volume spamming across a large amount of telephone numbers while attempting to avoid analytics engines. The two most common techniques involve either mimicking call patterns of a small to medium sized business and spreading calls over many phone numbers leased from VoIP wholesalers or spreading a very low volume of calls across a very large set of spoofed numbers.

Typically, the telephone numbers will have the same area code or local calling area to incite the consumer to answer. TNS has discovered a pattern to these calls and has proactively classified them as medium risk.

TNS has seen an increase of 52% in neighbor spoofing on a per subscriber basis from 1H2020 to 1H2021.

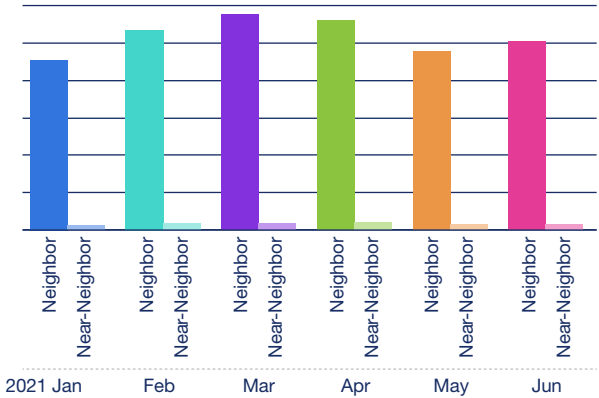
However, bad actors are using neighbor spoofing less due to implementation of STIR/SHAKEN on the major wireless networks. Instead, they have shifted to near-neighbor spoofing where the area codes are the same, but not the first five or six digits. TNS has seen a remarkable increase of 127% in near-neighbor spoofing on a per subscriber basis.

Near-Neighbor Spoofing Events per Subscriber



In addition, the call volume from near-neighbor spoofing numbers or legitimate telephone numbers from VoIP providers is over 30 times the volume compared to “pure” neighbor spoofing where the area code and exchange are the same.

Neighbor Spoofing vs. Near-Neighbor Spoofing



**Snowshoe Spamming** is a strategy where calls are propagated over several telephone numbers in low volume to avoid detection. The strategy is akin to how snowshoes spread the weight over a wide area to avoid sinking into the snow. Likewise, snowshoe spamming delivers its volume over a wide swath of telephone numbers to remain undetected.



**Near-neighbor spoofing continues to increase at over 125%**

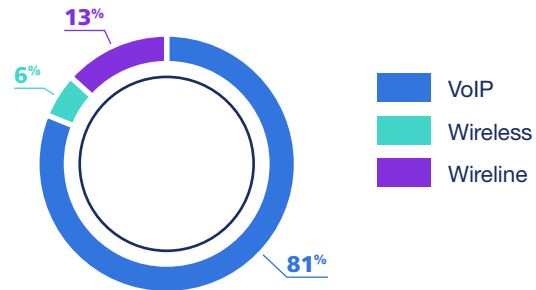
Snowshoe spamming is difficult to detect for over-the-top (OTT) applications. To be effective an application must be integrated with the network and see the cross-carrier events of both the calling number and the called number.

Without this tight integration, by time the OTT application determines the number to be from a bad actor, they have moved onto another number.

In the past, the hijacking of real wireless numbers was a consistent source and used primarily for neighbor spoofing. However, this trend appeared to shift to wireline numbers since STIR/SHAKEN has been deployed in the major wireless networks.

Near-neighbor spoofing shows that bad actors primarily use VoIP telephone numbers – over 80% of the call volume versus only 6% for wireless telephone numbers. The data is consistent from 2019 and December 2020.

### Near-Neighbor Spoofing by Line Type—1H2021

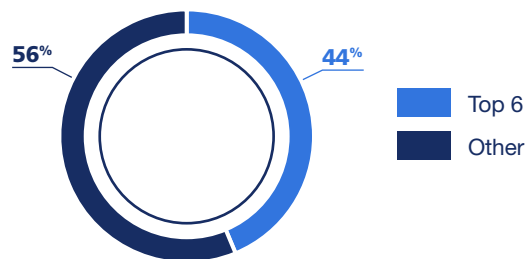


### STIR/SHAKEN Attested Traffic

STIR/SHAKEN authenticates the calling number but cannot address the question of intent. Still, this authentication framework is indisputably an essential foundational layer to combat spoofing. The FCC focused on larger voice service providers that have over 100,000 subscribers to implement STIR/SHAKEN by June 30, 2021.

However, the amount of cross-carrier traffic between the six largest US carriers (AT&T, CenturyLink, Comcast, T-Mobile and Verizon) account for less than half of the volume.

### Cross-Carrier Traffic Among Tier 1 Carriers



STIR/SHAKEN uses digital certificates, based on common public key cryptography, to ensure the calling number of a telephone call is secure. The originating service provider checks the call source and calling number to validate the calling number.

STIR/SHAKEN has a three-level system to categorize the essential information about the caller into levels of “attestation” for the call.

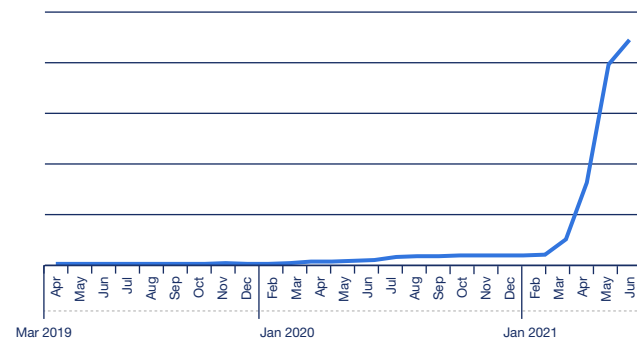
**Full Attestation (A)**—The service provider has authenticated the calling party and they are authorized to use the calling number.

**Partial Attestation (B)**—The service provider has authenticated the call origination, but cannot verify the call source is authorized to use the calling number.

**Gateway Attestation (C)**—The service provider has authenticated from where it received the call, but cannot authenticate the call source.

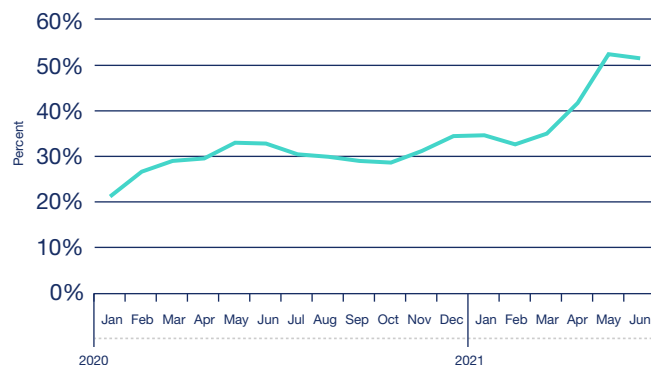
The amount of inter-carrier traffic that TNS has seen shows attestation has continued to grow dramatically in 1H2021.

### Inter-Carrier Signed STIR/SHAKEN Traffic



TNS estimates that call attestation has grown from 35% of the total traffic at the end of 2020 to over 50% by June 30, 2021.

### STIR/SHAKEN Traffic to Total Traffic



**STIR/SHAKEN needs to expand beyond the Tier-1 providers to have a significant impact**

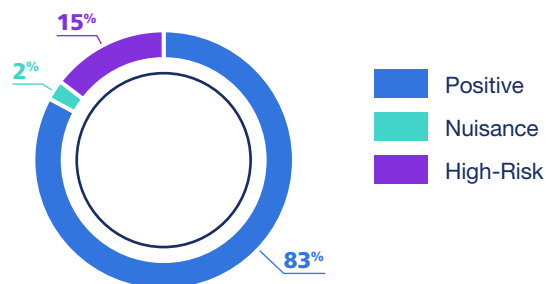
### Canadian Results

In April, the **Canadian Radio-Television and Telecommunications Commission (CRTC)** directed STIR/SHAKEN implementation by the end of November 2021. In addition, the Commission directs TSPs to file STIR/SHAKEN implementation readiness assessment reports by end of August and to add certain details to those reports.

TNS Call Guardian analyzes call events from Canadian telephone numbers across carriers every day and bases robocall scoring and categorization on this data.

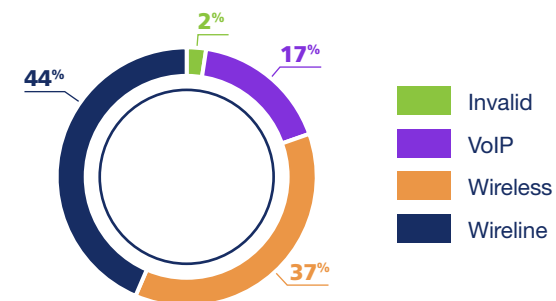
TNS found less than 20% of Canadian inter-carrier calls in 1H2021 were scored as unwanted, consistent with 2020 and 2019.

### Scoring by Category—Canadian Telephone Numbers—1H2021



Non-carrier numbers are 44% of the high-risk calls originating from Canadian telephone numbers in 1H2021 and consistent from 2020. TNS attributes this to US-based carriers blocking more invalid Canadian area codes.

### Distribution of Unwanted Calls from Canadian Telephone Numbers—1H2021



### International Results

TNS Call Guardian analyzes call events coming from international numbers and carriers and bases robocall scoring and categorization on this data.

The 1H2021 data shows 84% of calls from an international number as positive and significantly higher than previous findings.

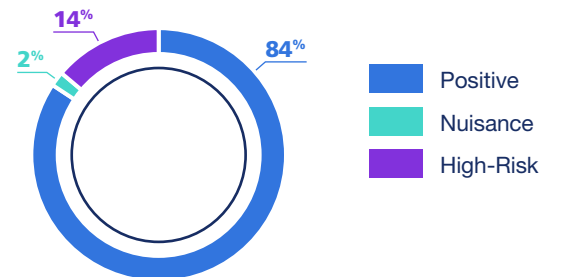
Many of the high-risk calls that come from international numbers are associated with **Wangiri** attacks.

The Wangiri scam designation comes from a Japanese term (where the scam originated years ago); it means one-ring-and-cut.

These scams typically have your phone ring once and the call stops. The bad actor then hopes you call the number back to see who it was or what it was about; once you do, you’ll hear a recorded message that is intended to keep you on the phone, or worse, to get you to call back a second time.

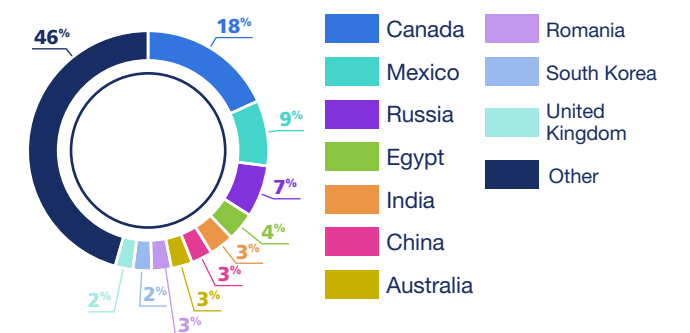
Every time you call, you will be charged high international rates or other connection fees. The bad actor profits from those fees.

### Scoring by Category—International Telephone Numbers



The top countries that have unwanted calls coming from their numbering resources are summarized below.

### Unwanted Calls from Numbers Outside US



**Note:** This data does not measure calls coming from an international gateway that spoofs a positive US-based number associated with an international number.



## The FCC voted in June 2019 to allow wireless carriers to automatically block unwanted robocalls for all subscribers, hoping that a shift from opt-in requirements would reduce the volume of incoming unwanted calls.

Addressing the rule approval, then-FCC Chairman Ajit Pai stated: “If there is one thing in our country today that unites Republicans and Democrats, liberals and conservatives, socialists and libertarians, vegetarians and carnivores, Ohio State and Michigan fans, it is that they are sick and tired of being bombarded by unwanted robocalls.”

Pai joined policymakers, carriers and industry stakeholders in taking more aggressive action on robocalls. While automatic call blocking may seem straightforward in policy and execution, there is a reason robocallers have been so difficult to reign in: they rapidly adjust tools, tactics and scams, making it difficult to discern unwanted from wanted calls.

These challenges help explain why only 39% of wireless subscribers want their carrier to automatically block all calls from numbers not in their mobile phone contact list.

For automatic call blocking to work, there are several factors and strategies that carriers should consider:

### Recognize Robocalls are Not Created Equal

Consumers are increasingly frustrated with the onslaught of robocalls; but all robocalls are not created equal in the minds and ears of consumers.

As referenced, less than 40% of wireless subscribers want their carrier or phone manufacturer to automatically block all calls primarily because they would have no knowledge a caller had tried to contact them.

However, consumers are much more amenable to have their wireless carrier automatically block calls when those calls are deemed high-risk (scam/fraud).

Almost 80% of consumers want their carrier to automatically block high-risk calls while letting others pass through so they can choose whether to answer, send to voicemail or block.

At the same time, most consumers still want to utilize voicemail for call screening. Almost 70% of consumers want lower-risk calls sent to voicemail, letting them control which messages to return.<sup>21</sup>

The takeaway for carriers, policymakers and regulators is that while consumers want protection from robocalls, they still want some control for less damaging nuisance calls.

### It's All About Data Analytics

Without trust in the underlying data, it is impossible for consumers to feel comfortable in ceding control in call blocking. Today, it is already possible to detect caller ID spoofing and other malicious and nuisance robocalling behavior based on real-time network data analytics.

However, when it comes to automatic call blocking, data analytics and machine learning are critical to determining with speed and accuracy which calls should be blocked and which ones to allow.

TNS' analysis of one billion calls per day across more than 500 telecom operators enables it to identify robocaller tactics and trends and to confirm which calls are legitimate; machine learning provides intelligence that can be applied to the data automatically.

This requires myriad data input into the machine learning. The simple act of identifying if an incoming call is from a scammer or a “wanted” robocall from, say, your child’s school or the pharmacy is a complex task.

Combining machine learning for accuracy and human analytics is necessary for effective automatic call blocking. Carriers must continue to employ trusted solutions to ensure the right automated call control decisions are made.

### Prioritize Consumer Education

Subscriber support for automatic call blocking requires a better understanding of how it works and how much control consumers will retain.

Consumers need to have confidence that important robocalls won’t be blocked by default, and that unwanted calls will not get through.

For carriers, this means clear and consistent communication to their subscriber base, educating them on which tools and technology are available and how they can employ them.

More than 70% of consumers surveyed agree that they would like to use an app from their wireless carrier to identify potential robocalls.<sup>22</sup> Ironically, the same percentage is not aware that such an app is offered. This is a red flag for more aggressive consumer education regarding the availability of this service/technology and the benefits these apps provide.

### STIR/SHAKEN is a Foundational Layer, Not a Silver Bullet

Carriers and handset manufacturers must consider how various types of calls are displayed on the phone once STIR/SHAKEN is fully deployed.

Apple’s adding STIR/SHAKEN support to iOS 13 suggests that the feature will be of limited value. iOS 13 users would only find out if a call is verified by scrolling through their call logs to see a checkmark icon on calls that already came through, rather than a real-time “Caller Verified”.

In this case, the onus is on consumers to go through call logs after-the-fact. However, a recent TNS study finds that even real-time call verification may not be enough to change consumer behavior. For incoming calls from an unknown number, a ‘*Telephone Number (TN) Validation Passed*’ icon did not lead to different call answer/block rates compared to just displaying the number.

Not surprisingly, eight in 10 people don’t answer a call from an unknown number even with a TN validation icon.

For those quick to judge the effectiveness of STIR/SHAKEN, consider that it took Firefox 17 years, 70 versions and 80% of webpages to be secure before it would mark websites as not secure. Similarly, it took Google 11 years and 68 versions.

The point is that building consumer confidence in a validation system, whether it’s secure/unsecure websites or validated/unvalidated incoming calls, is a long process.

Conversely, businesses can fully manage their voice calling brand; businesses and telemarketers have full flexibility to use branded calling to deliver their name, logo, and if desired, the intent of the call.

Automatic call blocking is part of a broader and necessary effort to more aggressively combat robocalls and shift much of the burden and associated frustration away from subscribers.

For the FCC rule to be implemented effectively by carriers, it is important to keep these factors in mind.



Seventy percent of consumers aren’t aware their wireless carrier has a robocall app



<sup>21</sup><https://tnsi.com/tns-robocall-survey-consumers-want-more-control-or-options-to-combat-robocalls/>

<sup>22</sup><https://tnsi.com/tns-robocall-survey-consumers-want-more-control-or-options-to-combat-robocalls/>

# Call originators making legitimate and wanted calls are seeing their businesses impacted by lower answer rates driven by consumer distrust of any unrecognized call.

Consumers, on the other hand, don’t realize the impact of what happens if millions of people let calls go unanswered or to voicemail. An ignored call from a telemarketer is just another missed robocall; but if the caller turns out to be the hospital informing you a family member has been injured or your child’s school calling with an important message, the stakes of ignoring calls become much higher.

Legitimate call originators, those businesses that rely heavily on contact centers and calling campaigns, are searching for a better way to get their calls answered without adding to the unwanted call burden for recipients.

Fortunately, there are a growing number of smartphone apps that categorize and provide a reputation for incoming calls to help combat robocalls. Many of these call authentication technologies provide consumers with additional caller information to distinguish between normal and nefarious calls and help consumers decide whether they should answer. With more context and verifiability should come a higher answer rate for legitimate incoming calls.

To enable this, call originators need to understand what tools are available to improve call validation and rectify the interaction with customers. Call authentication tools have varying levels of effectiveness driven by carrier network integration, the visibility the tool has into cross-carrier traffic and its ability to track and detect real-time spoofing events.

Calling parties may not always understand why their calls are being classified, so it’s important to equip legitimate call originators and consumers with intelligent tools to make informed decisions and avoid the risk of becoming a victim of scam or fraud.

For instance, the FCC recently made a declaratory ruling that will allow carriers to automatically block unwanted calls based on analytics when their customers are informed and can opt-out of the service.

More importantly, the definition of an unwanted call is extremely broad and can include calls with many customer complaints.

Call originators seeking to validate their calling campaigns via authentication analytics engines should consider the following best practices:

## Don’t Use One Main Calling Number for Multiple Uses

One common observation is that outbound numbers used for multiple purposes (e.g., by different departments) tend to get flagged by analytics engines and thus receive mixed feedback from consumers. A number used for marketing, for example, should not be used by other departments for other subjects.

Increased call frequency means that consumers will invariably provide negative feedback which leads to a robocall tag. By segmenting the use of toll-free numbers by purpose or subject, enterprises can improve their number’s status as legitimate.

## Use a Consistent, Real, Assigned Number and User-Dialable Calling Number

Bad actors will use invalid or unallocated telephone numbers. In November 2017, the FCC adopted new rules allowing providers to block telephone numbers they deem to be invalid, unallocated or unused.

However, on the carrier side, it is important to equip subscribers with as much relevant information about incoming calls as possible. Failing to display caller ID information could influence call authentication apps or network categorization frameworks while enabling bad actors to have better access to subscribers.

## Align Call Context and Content for the Duration of the Number’s Assignment

Consistently using the same number for the same purpose results in a more accurate reputation. As mentioned above, keep your numbers to single subject (department) to avoid being tagged as a robocall. When reassigning a number to another purpose best practice dictates that you wait 60 days before redeploying those numbers.

## Provide a Consistent Calling Name Profile that Matches Context

Displaying an accurate and consistent caller ID gives customers more confidence knowing who is calling and helps them make the decision to answer the call.

Consider using a service that can help you update and manage what is displayed on your outbound calls.

## Document Normal Calling Patterns

Call originators should inform analytics companies and service providers of their normal calling patterns, specifically with regards to time-of-day and the expected dialed volume.

When launching a new campaign, use a number that is compliant and “known”; this will aid analytics and service providers to designate the number as legitimate and not one being spoofed.

TNS offers a free website where call originators can provide feedback: [reportarobocall.com](https://reportarobocall.com). It includes the ability to bulk upload telephone numbers and provide any other relevant information that will ensure proper labeling.

Enterprises should work with analytics providers to register their calling campaigns



## Don’t Call Unassigned Numbers Frequently

Know your customers and their current numbers. Frequent calls to unassigned numbers are a red flag and mirrors a common, bad actor technique—dialing random numbers looking for unsuspecting consumers.

## Comply with DNC Lists, TCPA and FDCPA

Legitimate enterprises are willing to comply with state and federal laws such as the Do-Not-Call list, TCPA rules and Fair Debt Collections Practices Act (FDCPA). Bad actors, obviously, avoid this because it enables law enforcement to easily identify them.

## Branded Calling

Carriers and enterprises should evaluate enhanced enterprise tools like **Branded Calling**. To increase validation, and confidence in call identity, a corporate logo or other information is displayed to the consumer. This helps ensure businesses can reach their customers in an emergency; a prime example is if a doctor needs to contact a patient about their medical care.

There are also emerging solutions service providers can offer aggregators and enterprises with a lens into their call centers’ practices. The registration of calling campaigns, for example, could yield positive results as analytics engines better understand sudden spikes in calling traffic.

Call originators, service providers and other stakeholders throughout the telecommunications ecosystem recognize the risks associated with the rising tide of robocalls. Make no mistake, the correlation between consumer trust in voice calls and a customer’s faith in a business is inextricably linked. Lose a consumer’s trust and your brand will suffer.

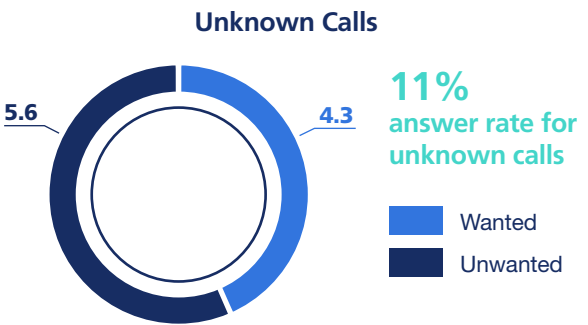
However, call originators that employ innovative solutions and embrace best practices will mitigate the impact of bad actor robocalls while ensuring a higher answer rate.

Improving your customer’s trust in your call authentication will help strengthen your brand.

## Branded Calling Study

TNS conducted a study in 2020 to understand the trust and behavior associated with incoming calls from enterprises. The goal was to determine how users react when no information is available about a caller. The study provided a baseline of user sentiment of enterprise calls and user expectations of a branded calling service.

On average, consumers receive approximately 10 unknown calls per week and only four of those calls are wanted. The answer rate for those unknown calls is just 11%.



Brand presence has strong effect on the consumer trust. Fifty-two percent of consumers say that seeing the brand on the incoming call has a strong effect on their trusting the call.

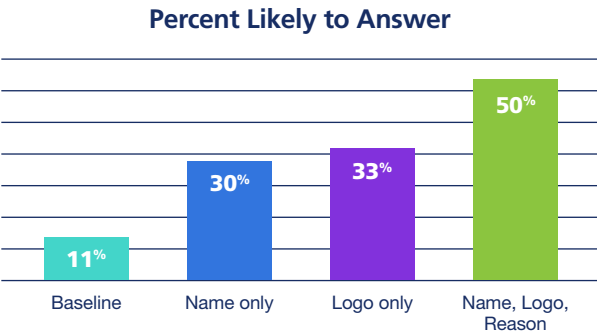
Consumers are most interested in receiving calls from healthcare services, financial institutions and delivery services.

## Consumers Most Interested in Calls From



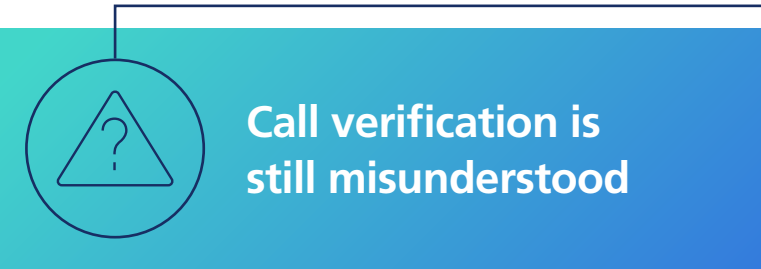
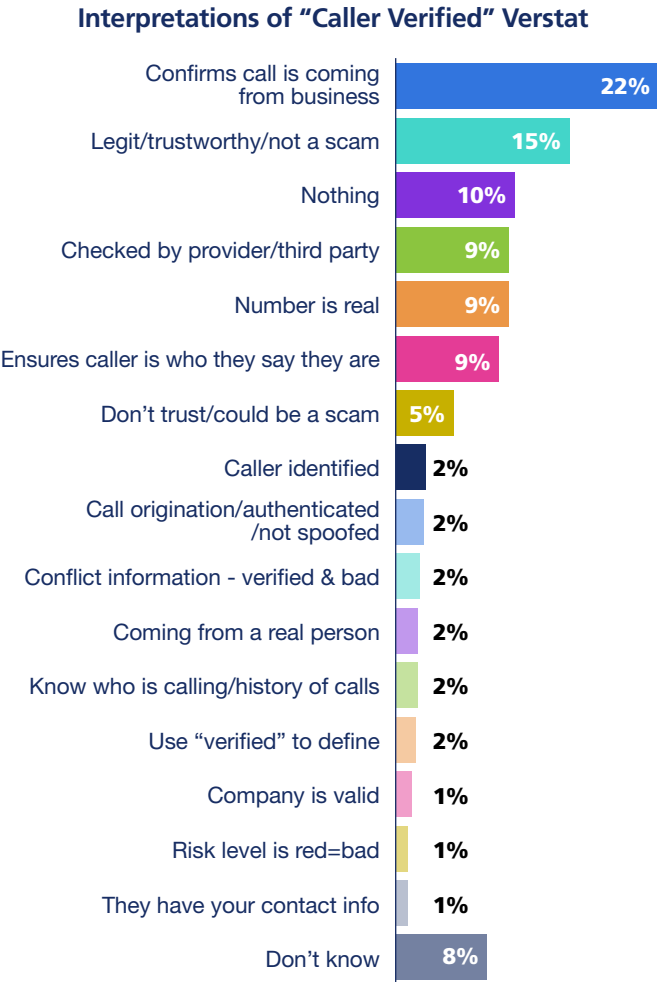


The content delivered to the consumer influences trust. Consumers are five times more likely to answer a call with brand presence than a simple phone number.

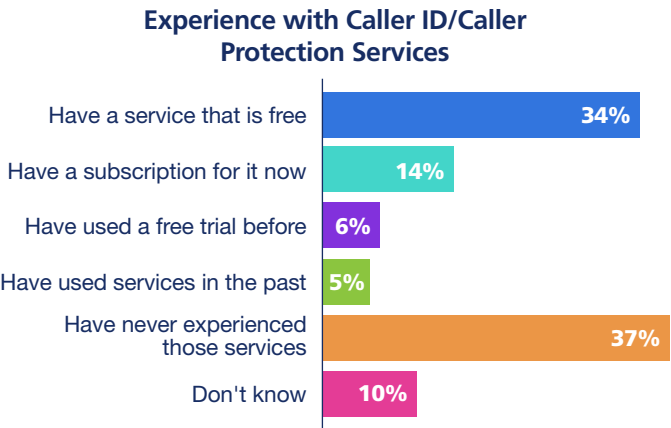


In general, consumers interpreted “caller verified” to mean the caller id correctly identified the number and it is, indeed, the business calling. This was also understood as being safe to answer.

Only 2% understood “caller verified” to mean the number was authenticated and not spoofed. The term meant “nothing” to 10% of consumers. There was also some confusion related to the presence of a risk level which was interpreted as negative and a potential scam risk.



Consumers are ready for branded calling and consumer acquisition and education are no longer an issue. Caller ID or Call Protection services are used by 54% of consumers.



# Regulatory Updates—2021

The FCC has been very focused on continuing the implementation of the TRACED Act in 2021 building off of the second half of 2020. This section focuses on just the first half of 2021.

You can refer to the [2021 Robocall Investigation Report, Sixth Edition](#) for the actions taken in the second half of 2020.

## Consumer and Governmental Affairs Bureau Announces Compliance Date for Remaining Reassigned Numbers Database Rule Regarding Reporting of Disconnect Data

In early February, The Commission released the **Reassigned Numbers Database Order**, establishing a database that will allow callers to determine whether a telephone number has been permanently disconnected. Beginning April 15, 2021 and recurring on day 15 of each month thereafter, service providers must report permanent disconnections of their subscribers.

The report must contain data for numbers permanently disconnected that were not submitted in the service provider’s prior reports. Notwithstanding the foregoing, small service providers (those providers with 100,000 or fewer domestic retail subscriber lines) have six additional months (until October 15, 2021) to begin reporting this information to the Reassigned Numbers Database Administrator.<sup>23</sup>

## FCC Issued a Notice of Proposed Rulemaking (NPRM) to Create a Limited Role for the Commission to Oversee Certificate Revocation Decisions

In Mid-February 2021, the FCC adopted and released an **NPRM** that seeks comment on to create a limited role for the Commission to oversee certificate revocation decisions by the private STIR/SHAKEN governance system that would have the effect of placing voice service providers in noncompliance with its rules.<sup>24</sup>

## FCC Calls on Carriers to Ensure Free Consumer Tools are Available to Block Robocalls and Issues New Robocall Cease-and-Desist Letters

On April 13, 2021, the Consumer and Governmental Affairs Bureau (CGB) wrote to major phone companies and issued a **Public Notice** to ask about what free robocall blocking tools they make available to consumers. In addition, the FCC’s Enforcement Bureau issued two more cease-and-desist letters to two phone service providers suspected of facilitating robocalls (R Squared and Phonetime Inc. dba Tellza). These companies market auto warranties and credit card debt reduction service and falsely claim to be from the Social Security Administration (SSA) or other well-known companies.<sup>25</sup>

## Robocall Mitigation Database Opens, Filing Instructions and Deadlines

On April 20, 2021, the FCC issued a **Public Notice** announcing that filings to a Robocall Mitigation Database were due on June 30, 2021, and that intermediate providers and terminating voice service providers would be prohibited from accepting traffic from voice service providers not listed in the RMD beginning September 28, 2021. Filers are able to request that any materials or information submitted to the FCC in their certifications be withheld from public inspection.<sup>26</sup>

## FCC Announced Letters to Carriers and Analytics Providers to Ask About Robocall Blocking Tools

Also, on April 20, 2021, the FCC sent letters to carriers and analytics providers to ask about robocall blocking tools.<sup>27</sup>

## FCC Announced a New Webpage to Collect TRACED Act Actions

The third action taken by the FCC on April 20, 2021 was announcing a new webpage to collect TRACED Act actions.<sup>28</sup>

<sup>23</sup><https://www.fcc.gov/document/cgb-announces-compliance-date-reassigned-numbers-database-rule>  
<sup>24</sup><https://www.fcc.gov/document/fcc-designates-robocall-traceback-manager>  
<sup>25</sup><https://docs.fcc.gov/public/attachments/DOC-371553A1.pdf>  
<sup>26</sup><https://www.fcc.gov/document/robocall-mitigation-database-opens-filing-instructions-and-deadlines>  
<sup>27</sup><https://www.fcc.gov/document/fcc-adopts-new-rules-combat-spoofed-robocalls>  
<sup>28</sup><https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts>

# FCC Releases Third Notice of Proposed Rulemaking for Promoting Caller ID Authentication to Combat Illegal Robocalls (WC Docket No. 17-97)

At the end of April 2021, the FCC released an **NPRM** to take further action in stemming the tide of illegal robocalls by proposing to **accelerate** the date by which small voice providers that originate an especially large amount of call traffic must implement the STIR/SHAKEN caller ID authentication framework.<sup>29</sup>

The NPRM would:

- Propose to shorten the extension for small voice service providers most likely to originate illegal robocalls by one year, so that such providers must implement STIR/SHAKEN in the IP portions of their networks no later than June 30, 2022
- Seek comment on how best to identify and define the subset of small voice service providers that that are at a heightened risk of originating an especially large amount of illegal robocall traffic
- Seek comment on whether to adopt additional measures, including data submissions, to facilitate oversight to ensure that small voice service providers subject to a shortened extension implement STIR/SHAKEN in a timely manner

One of the reasons for action is based on the *Robocall Investigation Report, Sixth Edition*, released by TNS in March 2021.

STIR/SHAKEN must be adopted in IP networks for large carriers by end of June 2021



## FCC (The Wireline Competition Bureau) Seeks Comment on Protective Order for Robocall Mitigation Database Collection

On May 10, 2021, the FCC sought comment on which parties should and should not ultimately be granted access to the confidential and highly confidential information included by voice service providers in their certifications.

<sup>29</sup><https://docs.fcc.gov/public/attachments/DOC-372025A1.pdf>

<sup>30</sup><https://www.fcc.gov/document/comment-sought-protect-order-robocall-mitigation-database-collection>

<sup>31</sup><https://www.fcc.gov/document/caller-id-authentication-governance-framework-revised>

<sup>32</sup><https://docs.fcc.gov/public/attachments/DOC-372307A1.pdf>

<sup>33</sup><https://docs.fcc.gov/public/attachments/DOC-372308A1.pdf>

<sup>34</sup><https://docs.fcc.gov/public/attachments/DOC-372827A1.pdf>

The FCC proposed only allowing access to limited categories of entities and individuals and only after such entities or individuals complete an appropriate process. The FCC proposed that entities or individuals that may seek to obtain access include federal, state, local and Tribal governmental entities involved in robocall enforcement; the registered industry traceback consortium; the STIR/SHAKEN Governance Authority; and intermediate providers and voice service providers who accept call traffic directly from a voice service provider listed in the database and request to review what actions that provider is taking to combat the origination of illegal robocalls.<sup>30</sup>

## WCB Announced Caller ID Authentication Governance Framework Revised to Enable Earlier Participation by Providers Without Direct Access to Telephone Numbers

Also on May 10, 2021, the WCB announced that the Secure Telephone Identity Governance Authority issued an update to its **Service Provider Code** (SPC) Token Access Policy to enable entities without direct access to telephone numbers to pursue the certification necessary to participate in STIR/SHAKEN caller ID authentication immediately after they have filed in the Robocall Mitigation Database.<sup>31</sup>

## FCC Issues New Robocall Cease-and-Desist Letters

On May 18, 2021, the FCC's Enforcement Bureau issued two more cease-and-desist letters to two phone service providers suspected of facilitating robocalls (**Prestige DR VoIP and VaultTel Solutions**). These companies market vacation packages and Social Security imposter scams.<sup>32 33</sup>

## FCC Proposes to Shorten Caller ID Authentication Deadline for Small Voice Service Providers Suspected of Originating Illegal Robocalls

On May 20, the FCC proposed and sought comment on shortening the amount of time afforded to certain small voice service providers for implementing caller ID authentication using the STIR/SHAKEN framework. New evidence indicates that a subset of small voice service providers are originating an increasing quantity of illegal robocalls.

The Commission additionally seeks comment on how best to identify and define the subset of small voice service providers that pose a heightened risk of originating an especially large amount of illegal robocall traffic. The Notice also sought comment on whether to adopt additional measures, including data submissions, to facilitate oversight to ensure that small voice service providers subject to a shortened extension timely implement STIR/SHAKEN.<sup>34</sup>

## FCC Concludes Assessment of Best Practices to Combat Unlawful Robocalls to Hospitals (CGB Docket No. 21-7)

On June 11, 2021 the FCC issued a **Public Notice** concluding its assessment of how the voluntary adoption by hospitals and other stakeholders of the best practices issued by the *Hospital Robocall Protection Group* (HRPG) can be facilitated to protect hospitals and other institutions from unlawful robocalls. The FCC concluded that education and outreach are the best ways to facilitate voluntary adoption of the best practices, and that organizations like the American Hospital Association (AHA) and other groups devoted to hospital risk management and security are in the best position to provide such outreach and training.<sup>35</sup>

## Wireline Competition Bureau Directs North American Numbering Council (NANC) to Issue Three Reports

The Wireline Competition Bureau directed the *North American Numbering Council* (NANC), via its *Call Authentication Trust Anchor* (CATA) Working Group, on June 15, 2021 to issue three reports:

1. No later than October 15, 2021, a report on **deployment of STIR/SHAKEN by small voice service providers** during the pendency of their extension from the STIR/SHAKEN implementation deadline
2. No later than February 15, 2022, a set of **best practices for how terminating service providers** can best protect their subscribers using caller ID authentication information
3. No later than June 15, 2022, recommending steps to encourage **adoption of caller ID authentication technology** and other techniques to combat robocalls by policymakers and providers outside of the United States.<sup>36</sup>

## Consumer and Governmental Affairs Bureau Announces Beta Test for Users of the Reassigned Numbers Database (CG Docket 17-59)

On June 11, 2021, the CGB announced the beta test period for the Reassigned Numbers Database ran July 1, 2021, through September 30, 2021. During this time callers and caller agents used the database without charge. According to the notice, the beta test enabled the administrator to determine appropriate subscription tiers and rates for the database when it is fully operational for paid users.<sup>37</sup>

<sup>35</sup><https://docs.fcc.gov/public/attachments/DA-21-688A1.pdf>

<sup>36</sup><https://www.fcc.gov/document/call-authentication-trust-anchor-cata-charge-letter>

<sup>37</sup><https://www.fcc.gov/document/fcc-announces-beta-test-users-reassigned-numbers-database>







## Hardware and Software

There are multiple hardware and software solutions available. Many products are limited to a single medium, such as traditional landlines or mobile phone contracts from a specific mobile phone operator.

Most OTT software solutions are not integrated with a carrier network and rely on the use of honey pots, blacklists and whitelists, which are not entirely effective.

## Blacklists and Whitelists

In its simplest form, this method offers the ability to prevent calls from phone numbers once they are known to be a source of robocalls. Many mobile apps can prevent robocalls with a user-generated blacklist.

A major problem for the use of both blacklists and whitelists is the practice of caller ID spoofing which is prevalent because of the low barrier to entry in VoIP services.

## Landline Call Blockers

For landlines there are standalone call blockers. Various models work on blacklist and whitelist principles and are not entirely effective, like OTT software solutions.

Several physical products have been developed for use with landlines. These are typically installed in homes and employ a hard coded or irregularly updated blacklist.

Some models also can create a user-generated whitelist<sup>38</sup>.

Newer devices for landlines can employ cloud-based data to resolve the hard-coded blacklist issues and allow you to create your own whitelist/blacklist.

## Crowdsourcing

Crowd-sourced feedback allows for an analytical layer. Supplementing the unstructured data provided by the machine learning methods, crowdsourcing provides more granular information, such as whether a telephone number is being used as a claim to offer free cruises or is a legitimate call from a bank with a fraud alert related to a credit card.

However, access to customer contacts can be problematic. OTT software require users to provide access to their personal whitelist of approved contacts, in exchange for access to the larger crowd-sourced database.

In 2013, hackers gained access to one OTT provider database of known genuine numbers, highlighting the danger of centralizing this information.<sup>39 40</sup>

## Do-Not-Originate

VoIP permits both legitimate and illegitimate caller name and number spoofing. Do-Not-Originate (DNO) involves the management of an outbound-calling blacklist consisting of the telephone numbers of financial institutions, government agencies, the 911 Do-Not-Call list, etc. used solely to receive inbound calls.

This DNO list will be checked by VoIP gateways as they process outbound calls.

The goal is to block call origination from numbers that should never originate phone calls. These numbers belong to entities such as the IRS, often used in caller ID spoofing, usually with the intent to defraud.

DNO could potentially allow the carrier to block any call that is using a non-allocated North American Numbering Plan NPA-NXX number.

On September 30, 2016, the FCC provided clarification that numbers added to the DNO list may be blocked by gateways.<sup>41</sup>

While implementation of DNO is straightforward technically, challenges remain in the creation, maintenance and security of the list server.

Once established, future additions to the list will have to be authenticated. The authority for provisioning this service will have to be established.

Finally, similar telephone numbers will not be included in the database and may still be used for fraudulent purposes.

## STIR/SHAKEN

While DNO is designed to prevent the origination of calls from telephone numbers that should not be making outbound calls, **STIR/SHAKEN** addresses identity authentication for calls traversing the Session Initiation Protocol (SIP) network to mitigate caller ID spoofing.

**STIR** (Secure Telephone Identity Revisited) can be used both to validate origination in real-time and to perform a traceback, after a call is complete.

STIR/SHAKEN is more complex than DNO. STIR defines a signature to verify the calling number and specifies how it will be transported in SIP “on the wire.”

**SHAKEN** (Signature-based Handling of Asserted information using toKENs) is the framework developed to provide an implementation profile for service providers implementing STIR.

STIR and SHAKEN use digital certificates based on common public key cryptography techniques ensuring the calling number of a telephone call is secure.

In simple terms, each TSP obtains their digital certificate from a trusted authority by other telephone service providers. The certificate technology enables the called party to verify that the calling number is accurate and has not been spoofed.

STIR may only be used to authenticate and validate origination of the call for US domestic calls and is applicable for SIP-to-SIP calls only. STIR is not applicable for Time Division Multiplexing (TDM), nor will it work if the network path of the call traverses a legacy network as opposed to an uninterrupted SIP-to-SIP call.

STIR/SHAKEN can attest to the authentication of the calling party telephone number but is not able to address the question of *intent*. Bad actors will be able to make malicious calls from numbers that have been assigned by a provider, and will be able to burn through those numbers, then move on to new ones to avoid detection.

STIR/SHAKEN is indisputably an essential foundational layer to combat spoofing. TNS also believes that it is crucial to understand its limitations and the ongoing need for the real-time analytics layer.

## Real-Time Analytics

Once fully deployed, DNO and STIR/SHAKEN will provide crucial layers of protection.

Among industry experts, however, consensus is clear a layered approach requiring access to an analytics server at the verification point is also required.

Today, it is possible to detect caller ID spoofing and other malicious and nuisance robocalling behavior based on real-time network data analytics. The analytics server uses advanced methods for blocking robocalls using real-time business intelligence techniques to address the constantly changing identities of robocalls.

With access to a large enough data sample, it is possible to create algorithms which detect unwanted robocall activity without depending solely on crowd-sourced reporting.

Advanced machine learning methods for blocking robocalls using real-time artificial intelligence (AI) in combination with big data gleaned from the network effectively addressed the constantly changing identities of robocallers. This methodology makes it possible to create an algorithm which can detect calling patterns without requiring crowd-sourced reporting.

Machine learning is a method used to devise complex models and algorithms that lend themselves to predictive analytics. The analytical models allow data scientists to produce reliable and repeatable decisions while also uncovering hidden insights through learning from historical relationships and trends in the data.

As an addition to this model, crowd-sourced feedback allows the analytics provider to layer in context.

Supplementing the unstructured data provided by the machine learning methods, crowd-sourced data allows the analytics layer to provide information at a more granular level.

## Enterprise Response to Analytics

TNS has observed a varied response among enterprises to the mitigation techniques that the industry has employed. Among the good actors, there has been a general willingness to adapt methodologies to conform with the analytics tools’ definitions of good behavior.



Branded calling can restore trust to the voice calling experience

The industry is implementing tools such as **Branded Calling**, where a logo and other business information may be displayed for legitimate calls.

Further, products that provide call origination aggregators and enterprises with a view into their call centers’ practices, such as **Telephone Number Reputation Monitoring** from TNS, allow them to understand how their numbers are being characterized, and when activity triggers unwanted reputational scores.

The registration of calling campaigns, for example, will yield positive results, as analytics engines better understand sudden spikes in calling traffic. TNS has seen a dramatic increase in the number of telephone numbers that enterprises have registered through the [Reportarobocall](#) website.

Specifically, one commonly observed trend is enterprises whose main outbound calling numbers are used for multiple purposes. These telephone numbers tend to get flagged by analytics engines and receive very mixed feedback from consumers. TNS recommends segmenting the use of toll-free numbers for various enterprise purposes. The registration of calling campaigns, for example, will yield positive results as analytics engines better understand sudden traffic spikes.

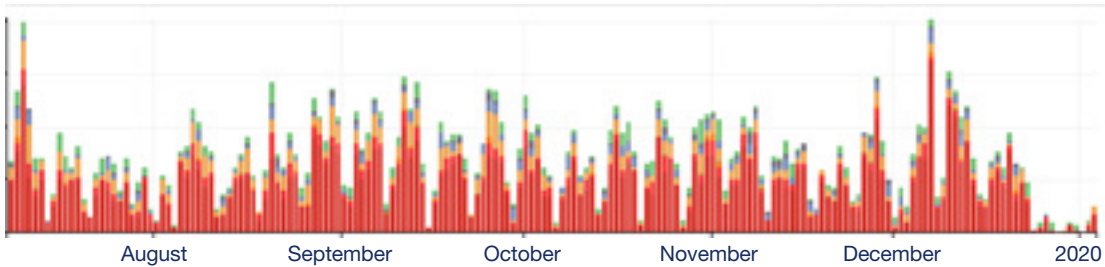
<sup>38</sup><https://www.consumerreports.org/cro/magazine/2015/07/robocall-blocker-review/index.html>

<sup>39</sup><https://blog.truecaller.com/2013/07/18/truecaller-statement/24>

<sup>40</sup><https://www.ehackingnews.com/2013/07/truecaller-database-hacked-by-syrian.html>

<sup>41</sup>[https://apps.fcc.gov/edocs\\_public/attachmatch/DA-16-1121A1.pdf](https://apps.fcc.gov/edocs_public/attachmatch/DA-16-1121A1.pdf)

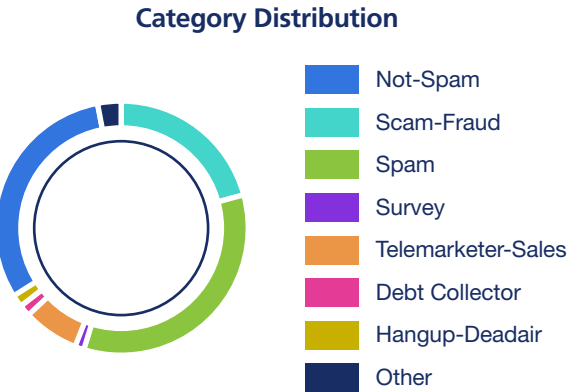




Above is an example showing mixed customer feedback.

The color of feedback corresponds to the color in the pie chart below, with blue being reports of scam-fraud.

These and other initiatives can restore trust to the calling experience.




**Customer feedback is often mixed when using a main calling number for multiple campaigns**



# Conclusions and Recommendations

## The FCC and CRTC continue exploration of methods to counter bad actors including blocking, adopting protocols to prevent number spoofing and tracebacks.

They have reached out to the service providers seeking the industry's help in their latest public notices to refresh the record on advanced methods to target and eliminate unlawful robocalls.

The goal of this report is to share data and analysis that proves helpful to the industry and robocalling efforts of TNS partners.


TNS publishes this report on a bi-annual basis to help the industry improve its security and detection to adapt to future situations.

Carriers and other industry experts involved in solving the robocall problem will be providing more detail about their approaches. Naturally, STIR/SHAKEN will play a significant role with respect to blocking and traceback efforts.

In addition, analytics providers will be explaining the complex role they play in solving this on-going scourge.

The industry will be looking to the FCC for guidance and support as it seeks to differentiate good calls from bad. More importantly, TNS will seek ways to support the FCC directives by onboarding data from vetted callers and facilitating traceback efforts. It is encouraging to see this problem coming into greater relief as the industry collaborates to re-establish trust in calling.

The robocall problem is more complex than it appears on its surface. There are many solutions to combat robocalling, however, a layered approach will continue to be most effective. This strategy includes the work being done to implement STIR/SHAKEN and the policy and structure around DNO.



**A layered approach is most effective in combating robocalls**







**Transaction  
Network Services**

**To find out how TNS can help your  
organization combat Robocalls:**

+ 1 703 453 8300 | [solutions@tnsi.com](mailto:solutions@tnsi.com) | [tnsi.com](https://tnsi.com)

©2021 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, and Call Guardian Authentication Hub are registered trademarks of Transaction Network Services