



# 2022 Robocall Investigation Report

## Eighth Edition

By Transaction Network Services

March 2022

# Table of Contents

---

## 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

**23**

---

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

**25**

---

## Regulatory Updates—2H2021

**28**

---

### Industry Solutions to Combat Robocalling

**32**

---

## Conclusions and Recommendations

**35**





## The TNS 2022 Robocall Investigation Report, Eighth Edition (Robocall Report) is a continuing examination into the data, convention and trends that plague consumers' phones daily.

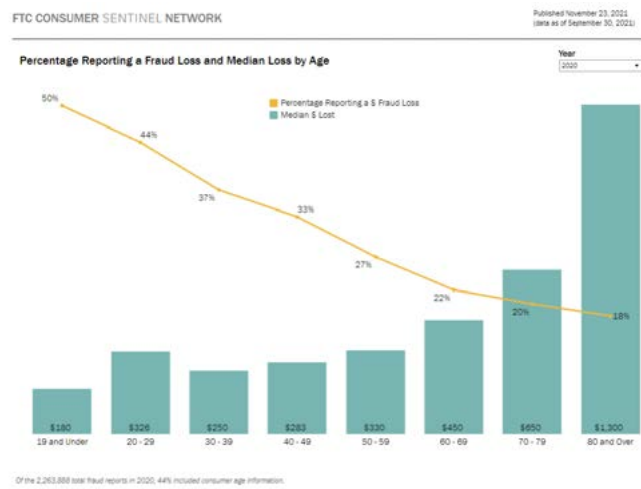
**TNS' Call Guardian®, the industry-leading big-data analytics engine, has gained insights and reputation data on almost two billion active phone numbers by analyzing over 1.5 billion daily call events across hundreds of carriers.**

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

- **Robocalls were slightly up in 2021.** Unwanted calls increased 2% in 2021 (78.9 billion) compared to 2020 (77.2 billion). Compared to 2019 (106.8 billion), unwanted calls are down significantly (-26%). Despite the drop, only 38% of consumers in a recent TNS survey felt they received fewer robocalls during the pandemic than before COVID-19.
- **Pandemic highlights need for branded calling.** Struggles by health agencies to reach Americans with critical COVID-19 information during the pandemic has exposed the lack of consumer trust in voice calling and the need for branded calling. Forty-three percent of consumers still answer calls from unknown numbers for fear of missing an important call, which is why nearly six in 10 (59%) of those surveyed would answer a call if the caller ID displayed the logo of a brand they recognize.
- **Tier-1 carriers continue to be a small part of the problem.** Seventy-three percent (73%) of inter-carrier traffic originates from Tier-1 carriers; however, more than 95% of high-risk calls originate from non-Tier-1 telephone resources.
- **Robocallers crossing over to robotexts.** With STIR/SHAKEN improving call authentication across networks, robotexts are a logical way for spammers to work around that new standard. TNS found that in December 2021, 48% of robotext scams were from a robocall spammer.
- **VoIP originated calls are the largest portion of unwanted calls.** Over two-thirds (68%) of all high-risk calls and 73% of all nuisance calls originate from VoIP numbers – representing the largest two sources of these unwanted calls.
- **Wireline phone numbers overlooked as robocaller target.** While much of the attention is focused on robocalls to mobile phones, almost half (48%) of inter-carrier calls placed to wireline numbers in 2021 were unwanted, compared to 21% of inter-carrier calls to wireless numbers.

Industrywide,

- Consumers lost more than \$3.5 billion to fraud in the first three-quarters of 2021 – an increase of nearly \$1.7 billion over 2019.<sup>1</sup>
- Imposter scams topped the list of consumer complaints submitted in 2021 in terms of number reported and total dollar loss to the Federal Trade Commission's (FTC) nationwide Consumer Sentinel; investment related fraud was second on the list in total dollar loss followed by online shopping as the third highest total. These top three scams account for 82% of the total dollar loss according to the FTC.<sup>2</sup>
- The FTC saw a 24% increase in complaints to the Do-Not-Call Registry received when comparing January-September of 2021 to the same period in 2020.<sup>3</sup>
- Younger people reported losing money to fraud more often than older people. In first nine months of 2021, 50% of people 19 and under reported a loss to fraud, while only 18% of people in their 70s.<sup>4</sup>
- However, when people in their 80s did lose money, the amount tended to be higher: their median loss was \$1,300, compared to \$326 for people in their 20s.<sup>5</sup>



<sup>1</sup><https://public.tableau.com/app/profile/federal.trade.commission/viz/TheBigViewAllSentinelReports/TopReports>

<sup>2</sup><https://public.tableau.com/app/profile/federal.trade.commission/viz/TheBigViewAllSentinelReports/TopReports>

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

<sup>4</sup><https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/AgeFraudLosses>

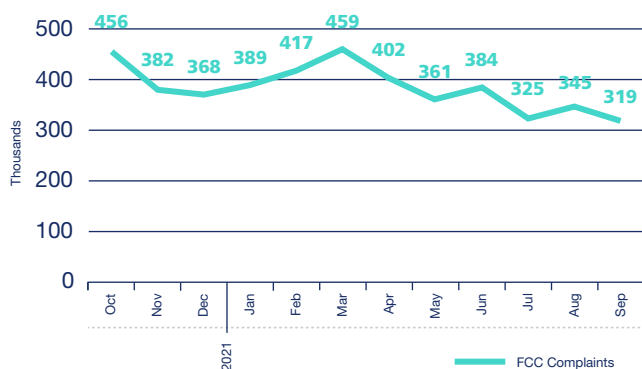
<sup>5</sup><https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/AgeFraudLosses>

## Fraud amounted to \$3.5 billion through September 2021



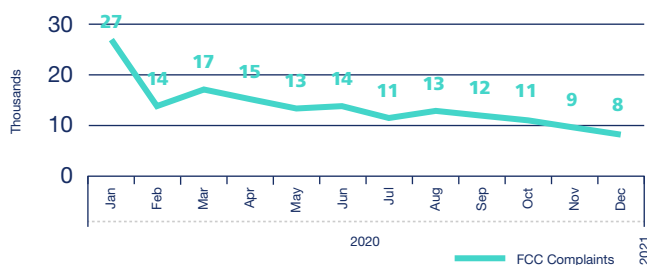
Fraud has become easier for criminals as technology, like VoIP calling, has enabled both spoofing numbers and low cost robo-dialing. A late 2021 TNS study found 43% of consumers still answer calls from unknown numbers for fear of missing an important call, which is why nearly six in 10 (59%) of those surveyed would answer a call if the caller ID displayed the logo of a brand they recognize.

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



- However, the FCC saw a decrease in in complaints to the Don-Not-Call List of 8% when comparing 2021 to 2020.<sup>9</sup>

### FCC Complaints—Last 12 Months



- Carriers are doing a better job of blocking these calls. Carriers also have made low-cost tools available to their wireless subscribers and have educated them on robocalling.

### 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. *Unwanted* represents non-positive calls or those that are scored as nuisance or high-risk.



**Nearly 80 billion  
unwanted calls in  
last 12 months**

The TNS 2022 Robocall Investigation Report, Eighth Edition is a continuing examination into the trends published in the 2018, 2019, 2020 and 2021 Robocall Reports. Call Guardian, the industry-leading big-data analytics engine, has gained insights and reputation metrics on almost two billion phone numbers by analyzing over 1.5 billion daily call events across hundreds of carriers.

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

Billions of data points weave together 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 and robotexting**.

<sup>9</sup><https://opendata.fcc.gov/Consumer/Consumer-Complaints-Data-Unwanted-Calls/vakf-fz8e/data>

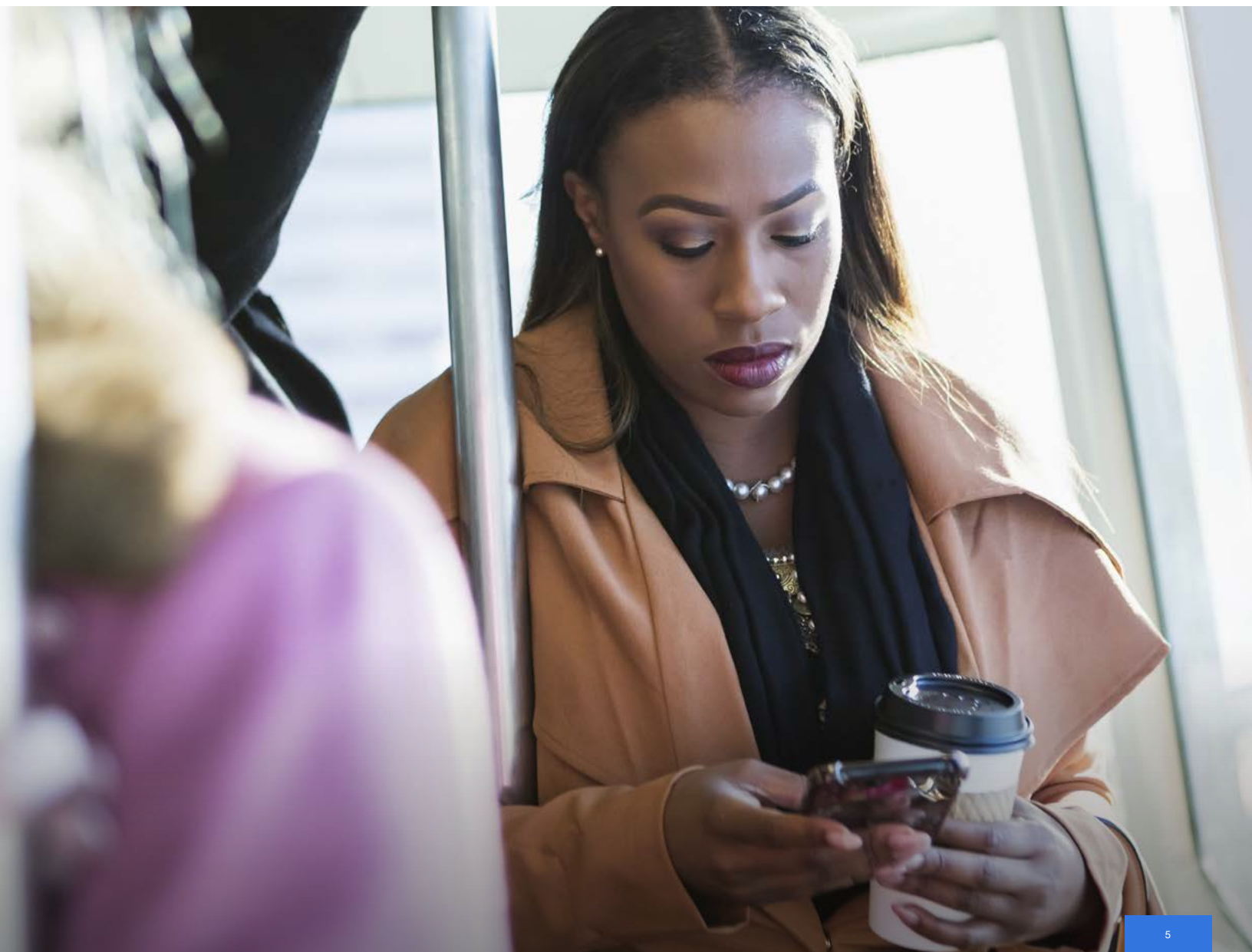
## ***The TNS 2022 Robocall Investigation Report, Eighth Edition* includes a vast amount of factual evidence derived from real network traffic since 2018.**

**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.



# Primer on Robocalling

The *Telephone Consumer Protection Act* or 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 that contain a message made with a prerecorded 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 from 2019.<sup>8</sup>

However, the lists have been ineffective. While legitimate callers 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>

<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/7546510/>





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

Call Guardian analyzes over 1.5 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 honeypots 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 to project reputations on virtually any telephone number (TN).

Call management and caller ID applications are designed to protect legitimate phone callers (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 help 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.

TNS Network  
Data Sources

Results of  
Over Billions  
of Signaling



Database Transactions  
per Day from Over  
500 Operators

### 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



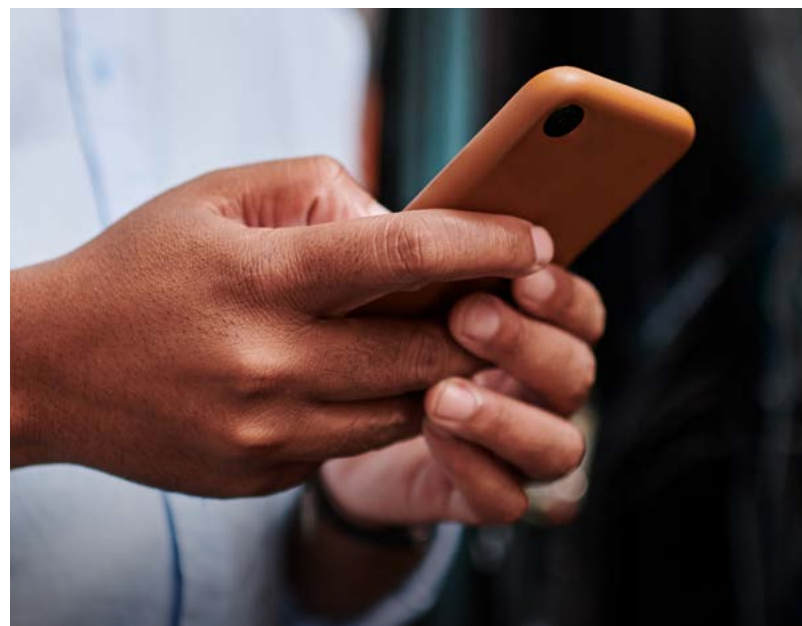
STIR/SHAKEN Parameters



Fraud, Spam and Premium Rate Called Numbers



Machine Learning Algorithm—Real-Time Scoring of 1.9B TNs



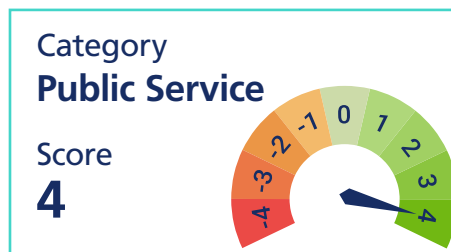
# Results and Analysis

## Reputation Category and Scoring

TNS uses reputation categories to score common call behavior. This reputation scoring is comprised of categories that 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. These callers are preying on consumers and have one of the following characteristics:

- Knowingly and willfully causing transmission of misleading or inaccurate caller ID info for which there is suspicious behavior indicative of malicious intent, which otherwise would cause potential fraud.
- Appear to be in reckless disregard of state and federal laws governing the use of auto-dialers or a person using an auto-dialer in the commission of a crime of identity theft or fraud.

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.

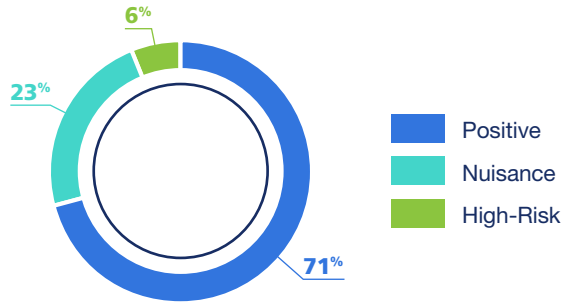
**Credit card interest scams**

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



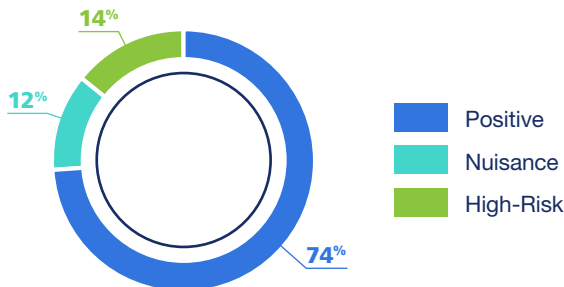
TNS found that 29% of the inter-carrier calls in 2021 were scored as *unwanted*, consistent with 2020, but slightly higher which says the problem isn't going away.

### Scoring by Category—2021



The past year 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 23% for all of 2021 and only 20% in first half of 2021.

### Scoring by Category—2020

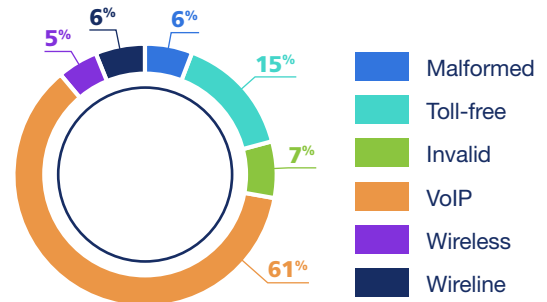


## Origination of Unwanted Calls

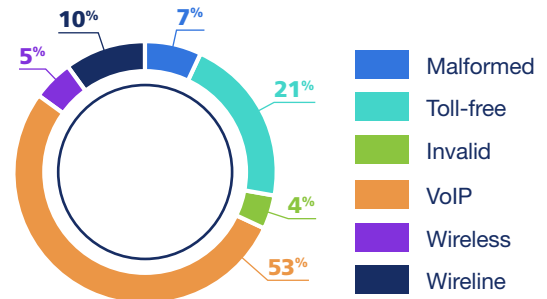
VoIP calls represent telephone numbers utilized by the cable operators (MSOs) and VoIP providers.

VoIP calls accounted for 61% of the unwanted calls in 2021 by total volume, up significantly from 53% in 2020. Toll-free calls were the second highest at 15%.

### Distribution of All Unwanted Calls—2021



### Distribution of All Unwanted Calls—2020



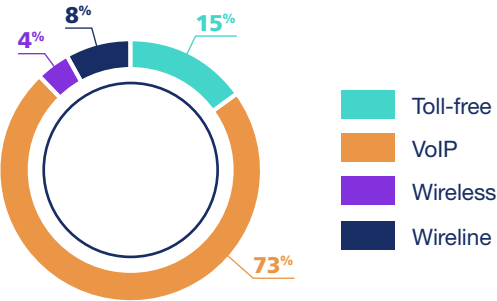
Providers that allow users to bring their own device and unbundle service so that direct inbound numbers may be purchased separately from outbound calling minutes are another source for bad actors.

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 73% of the calls in the first half of 2021.

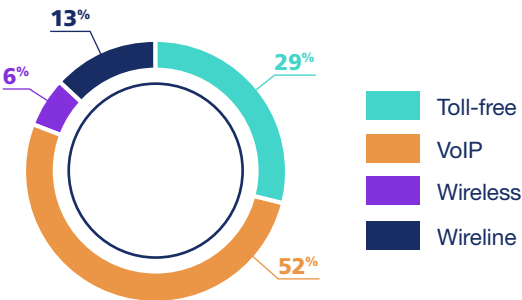
Distribution of Nuisance Calls—1H2021



VoIP calls are nearly three-quarters of the nuisance calls



Distribution of Nuisance Calls—2020

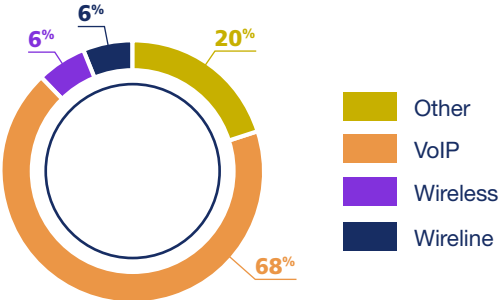


VoIP numbers, in 2021 remain the largest source (68%) of high-risk calls, up significantly from 54% in 2020. Invalid and malformed numbers are in the “other” category along with toll-free numbers and are the second highest source of high-risk calls in the charts below.

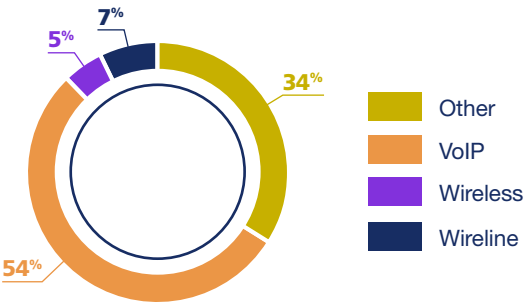
While there are legitimate reasons to modify the calling number, bad actors use this technique to hide their identity.

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.

Distribution of High-Risk Calls—2021



Distribution of High-Risk Calls—2020



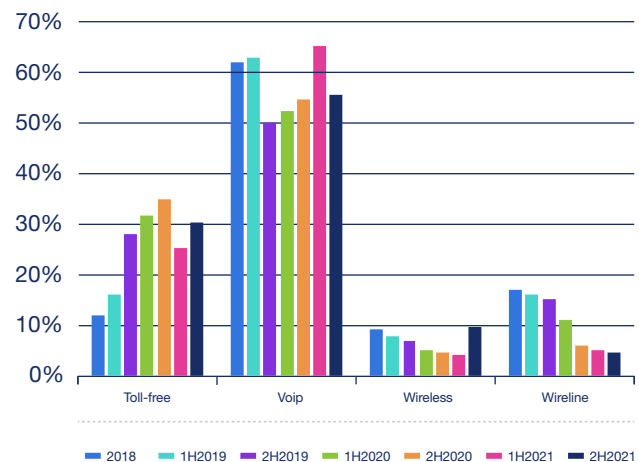
Spoofing of wireless telephone numbers had been declining from 2020 to 1H2021, however it increased in the second half of 2021. Bad actors have shifted to near-neighbor spoofing where the area codes are the same, but not the first five or six digits which is being done primarily by VoIP numbers.

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

Bad actors appear to have shifted from originating calls utilizing toll-free numbers to VoIP numbers. Unwanted, high-risk calls from VoIP numbers jumped to 68% in 2021 from 55% in 2H2020, as you can see from the chart below. Toll-free numbers, however, continue to rank as second highest and saw an increase in the second half of the year. The increase is due to the use of high-volume spamming of donation calls for police, firefighters and breast cancer awareness.

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 their [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.

**Distribution of High-Risk Calls Over Time**



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 and approved 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, for non-facilities-based providers. The FCC will further require any small voice service providers that the Enforcement Bureau suspects of originating illegal robocalls and that fails to mitigate such traffic upon Bureau notice or otherwise fails to meet its burden under section 64.1200(n)(2) of its rules, to implement STIR/SHAKEN within 90 days of that determination unless sooner implementation is otherwise required.<sup>11, 12</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.

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 5% of the high-risk calls in 2021 originated from the top seven carriers (AT&T, CenturyLink, Charter, Comcast, T-Mobile UScellular globally and Verizon). This is a significant drop from 11% in 2019 and down from 6% in 2020.

**Beware of fraudsters targeting police and firefighter donations using toll-free numbers**

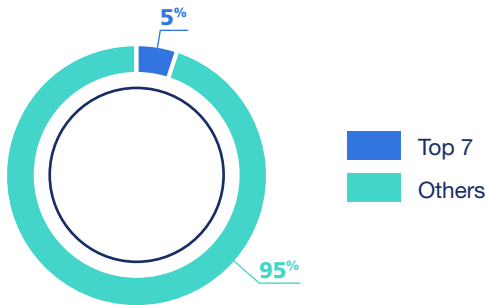


<sup>11</sup><https://docs.fcc.gov/public/attachments/FCC-21-62A1.pdf>

<sup>12</sup><https://www.fcc.gov/document/fcc-moves-small-provider-stirshaken-start-date-combat-robocalls-0>

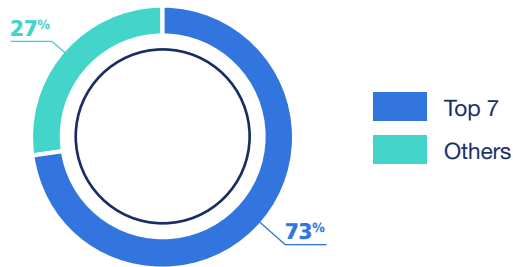


### Telephone Numbers Placing High-Risk Calls—2021



The Tier-1s account for 73% of the total number of calls in 2021, up slightly from 67% in 2020. However, the Tier-1s are a declining percentage of high-risk calls.

### Telephone Number Resource Total Calls—2021



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

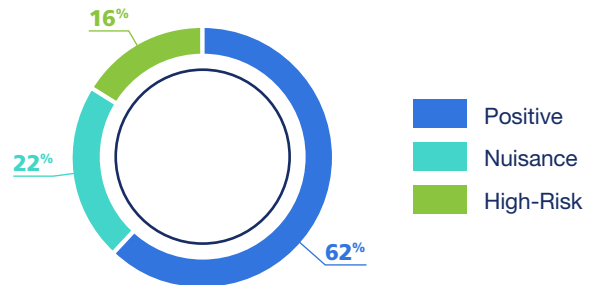


VoIP networks make it relatively easy to spoof caller ID. While most unwanted calls continue to originate from VoIP numbers, the percentage of unwanted VoIP calls went up to 38% in 1H2021, more than double from 2020 (17%).

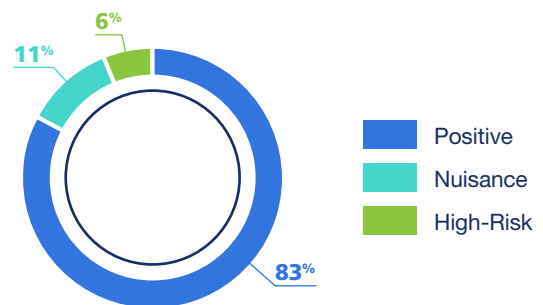
TNS believes this is due to low-volume spammers using VoIP to generate robocalls that are being purchased by wholesale VoIP providers.



### Scoring of VoIP Telephone Numbers—2021



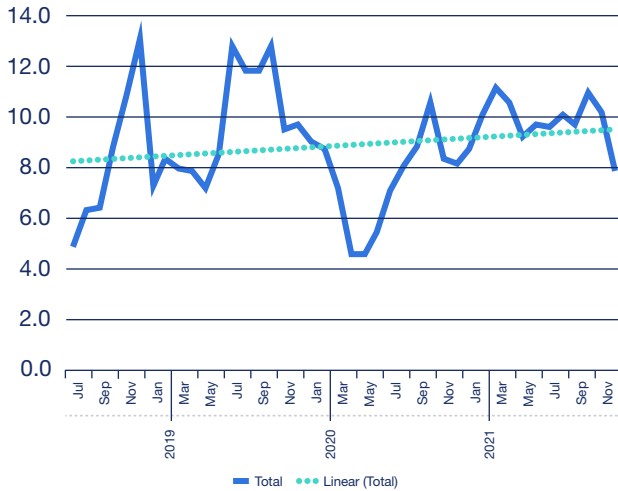
### Scoring of VoIP Telephone Numbers—2020



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

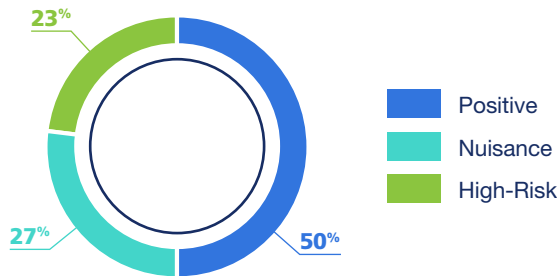
Bad actors are using VoIP networks to originate calls. The number of nuisance calls, on a per subscriber basis, coming from a VoIP number, has stayed relatively flat to slightly declining. However, the number of high-risk calls, per subscriber, has more than doubled, up 123% in comparing 1H2021 to 1H2020.

### Unwanted Calls per Telephone Number—VoIP

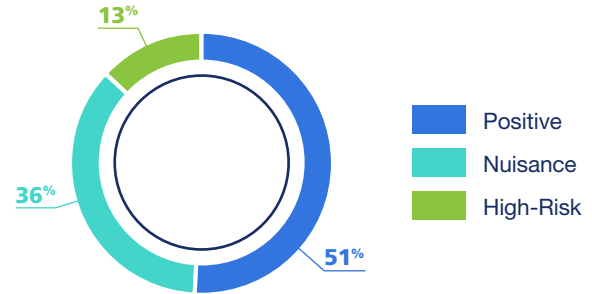


The percentage of unwanted calls coming from toll-free numbers was similar with 49% unwanted in 2020 to 50% in 2021.

### Scoring Distribution of Toll-Free Calls—2021



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

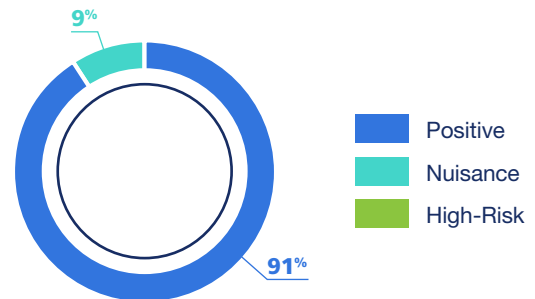




**Top 10 toll-free calls have moved to high-risk from nuisance**

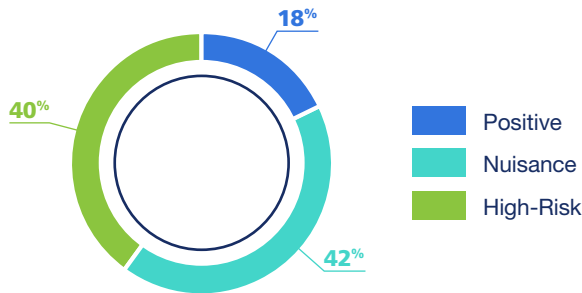
Of the top 10 toll-free numbers in 2021 in terms of call volume, 91% of the calls are scored as positive from TNS, up from 71% in 1H2020. This jump is due to an increase in enterprise and government agencies registering toll-free numbers.

### Scoring of Top 10 Toll-Free Telephone Numbers by Volume—2021



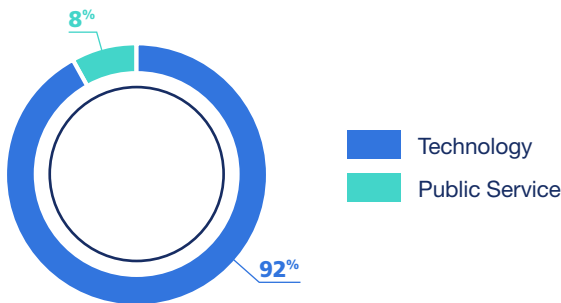
The crowd-sourced data from the top 10 toll-free numbers, however, is overwhelmingly considered nuisance or high-risk by the subscriber.

**Crowd-Source Sentiment of Top 10 Toll-Free Telephone Numbers—2021**



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 Telephone Numbers by Volume—2021**



The perceived risk of missing an important phone call was heightened during the COVID-19 pandemic in 2020 and 2021. For example, one of the biggest challenges contact tracers faced – especially in the early months of the pandemic – was an unexpected one: robocalls. Scammers spoofing legitimate government and health agency phone numbers tricked people into surrendering money or personal information. The fact is 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 prioritized efforts to authenticate call identification information for consumers and improve answer call rates for legitimate contact tracing calls.


The challenge faced by contact tracing efforts is simply the latest – albeit higher stakes – manifestation of the extent to which 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 if the call has not been verified as coming from that call originator. 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 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 and the need to communicate other time sensitive medical and health information, policy, telecom and industry leaders are taking steps to help boost trust in voice calling. Branding incoming calls has shown to increase consumer 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.



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

<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)



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.

ATIS announced two policy changes in the SHAKEN ecosystem during the summer of 2021. The set of first policy changes will allow delegate certificates to be used by third-party callers as well as companies originating calls from toll-free numbers to also provide SHAKEN authentication.<sup>14</sup>

A delegate certificate gives service providers a method to establish a customer's right to use a telephone number when the service provider did not assign that number itself. The use of a delegated certificate enables calls to receive the highest level of attestation when a company sends an outbound call through one service provider using a number assigned to it by another service provider.

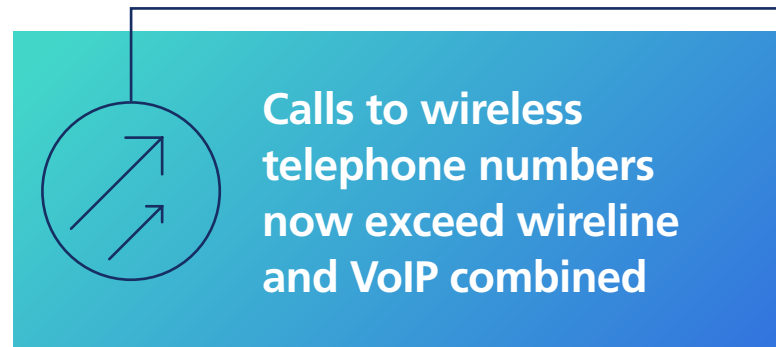
A RESPOG is the entity that assigns a toll-free number to a customer and is the only entity that can authenticate that a customer has the right to use a toll-free number. Unless a Resp Org is also a service provider, it is not involved in originating a call and previously was not able to provide the SHAKEN authentication. The policy revisions will afford companies sending traffic outbound from a toll-free number the means to qualify for the highest level of attestation.

In addition, ATIS is working on standards for Rich Call Data (RCD) which is intended to provide more information to help wireless subscribers to understand whether they want to answer phone calls. RCD would show caller name, logo image and other optional information. RCD is part of the STIR/SHAKEN framework. It is included in the SHAKEN Identity token and is digitally signed using Public Key Infrastructure (PKI). This makes RCD a more accurate and trusted means of presenting caller information. In the absence of such widely deployed standard, leading carrier led analytics and mobile application companies are enabling richer call display with innovative pre-RCD solutions.



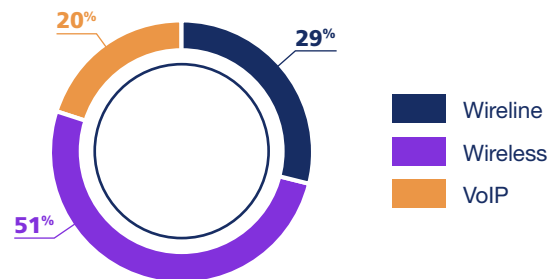
## Termination of Unwanted Calls

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.



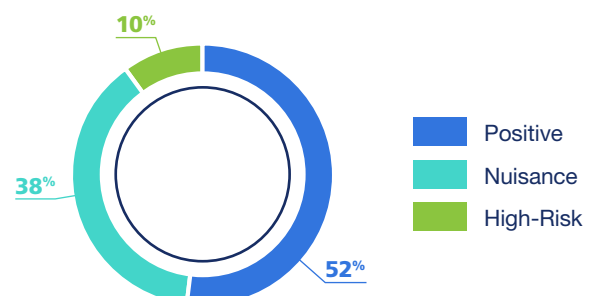
Calls to wireless telephone numbers account for 51% of the total call volume for 2021, up from 46% in 2020. Call volume to wireline has decreased 6% while call volume to wireless has increased 16% comparing 2021 to 2020.

**Total Call Distribution  
Called Telephone Numbers—2021**



While much of the attention goes towards robocalls to mobile phones, TNS finds that 48% of wireline calls in 2021 were unwanted, compared to 21% to wireless numbers.

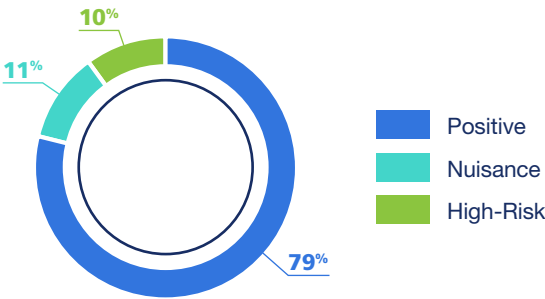
**Distribution of Scoring for Wireline  
Telephone Numbers—2021**



<sup>14</sup><https://www.atis.org/press-releases/sti-ga-announces-policy-changes-to-support-delegate-certificates-and-toll-free/>

Unwanted 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—2021



Almost 50% of the calls to wireline are unwanted



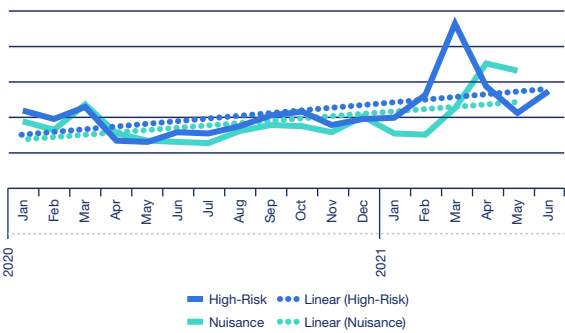
The percentage of unwanted calls to wireline numbers dropped 4% when comparing 2021 to 2020. This is consistent with the overall decrease in total wireline call volume. However, unwanted calls to wireless numbers increased by 59% in this same period mostly because of COVID-19 and a drop in calling volume from April through June 2020.

Both wireline and wireless high-risk calls declined in 2020 but the number of nuisance calls increased. Wireline nuisance calls increased 105% while wireline high-risk calls decreased 54% in 2021. At the same time, wireless nuisance calls increased 143% while high-risk calls decreased 22% 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.

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, CenturyLink, TDS Telecom, T-Mobile, US Cellular, Verizon and Vonage, all of which offer free blocking services, often through a third-party analytics company.<sup>15</sup>

<sup>15</sup><https://docs.fcc.gov/public/attachments/DA-21-772A1.pdf>

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 *Scam Shield*, which includes caller ID and several other features at no additional cost
- 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
- CenturyLink offers VoIP customers 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*

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



**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. Call Guardian is the underlying technology for Call Guard and uses industry-leading data, STIR/SHAKEN.

**Comcast** has a new caller ID verification tool, Xfinity Voice Spam Blocker, 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. Call Guardian is part of the underlying technology for Xfinity Voice Spam Blocker.

**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.

**CenturyLink** 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, CenturyLink performs DNO blocking of government impersonation.

**TDS Telecom** uses 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.

**US Cellular** offers call blocking through 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. US Cellular’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 US Cellular subscribers.



**Verizon**, at the network level, has blocked hundreds of millions of calls across-the-board where the calling number is invalid, unassigned or determined to be high-risk by the analytics engine, 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>16</sup>

## Top Scams

There are different tactics that criminals use to defraud millions of people 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 can include asking the caller for a name, company, street address, telephone number and professional license number.

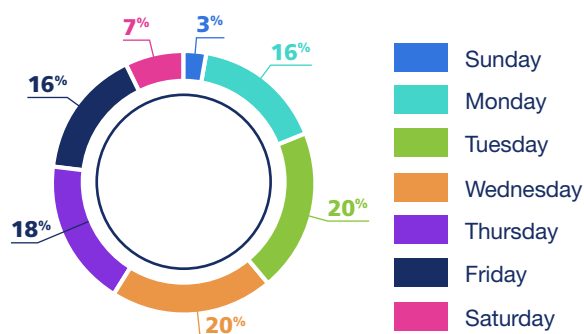
**Home buying scam**—The scams begin by asking what kind of property you own and if you are interested in selling it, attempting to make the call sound legitimate. Then they will make a bogus offer, possibly one you cannot refuse. The catch – there is an “administrative fee” which, after being paid, 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 (20%) occurred on Tuesdays and Wednesdays during 2021. The weekend represented 10% of total calls, a slight decrease from 14% in 2020.

**Distribution of All Unwanted Calls—2021**



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.

Fraudsters may pose as a legitimate charity, make up a fake organization name that sounds trustworthy or even create a registered charity but misuse funding.

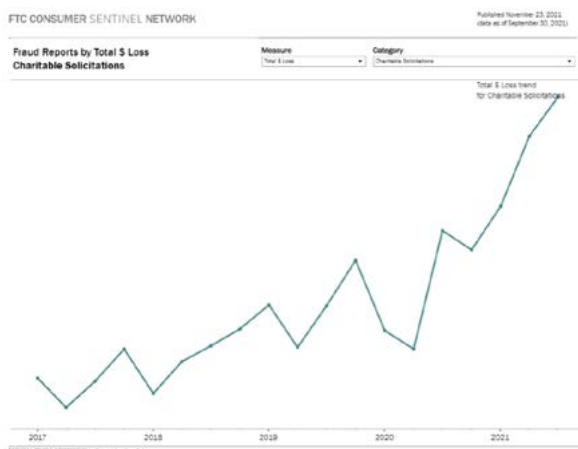
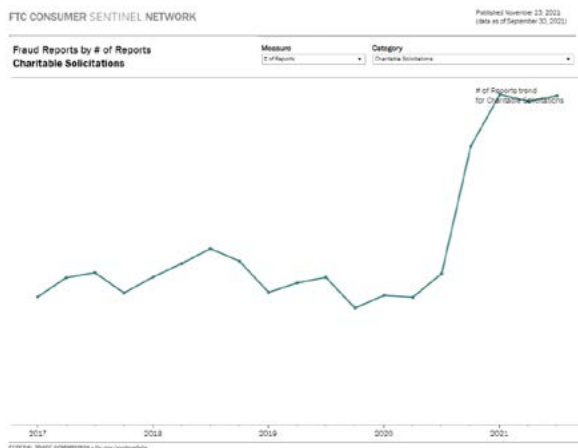
<sup>16</sup><https://www.fcc.gov/document/call-blocking-report-tools-now-substantially-available-consumers>

## Donation Scams

The FTC has received 6,864 fraud incident reports for charitable contributions totaling \$10.9 million in the first quarter of 2021.<sup>17</sup>



The total number of reports and dollar loss submitted to the FTC grew dramatically in 2021.<sup>18</sup>



The FTC provides important questions to ask a caller regarding the charity including:<sup>19</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>20</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

## Robotext Scams

On October 18, 2021 FCC Acting Chairwoman, Jessica Rosenworcel, shared with her colleagues a proposed rule that would require mobile wireless providers to block illegal text messaging, building on the agency's ongoing work to stop illegal and unwanted robocalls. As the FCC continues to combat unwanted robocalls, it recognizes that it must adapt to the latest scamming trends—including the rise of robotexts. If adopted by a vote of the full Commission, the rulemaking would explore steps to protect consumers from illegal robotexts, including network level blocking and applying caller authentication standards to text messaging.

In 2020 alone, the FCC received approximately 14,000 consumer complaints about unwanted text messages, representing an almost 146% increase from the number of complaints the year before. Through the first three quarters of 2021, the Commission received over 9,800 consumer complaints about unwanted texts. As the FCC continues to combat unwanted robocalls, it recognizes that it must adapt to the latest scamming trends—including the rise of robotexts.

<sup>17</sup><https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts>

<sup>18</sup><https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts>

<sup>19</sup><https://www.consumer.ftc.gov/articles/before-giving-to-charity>

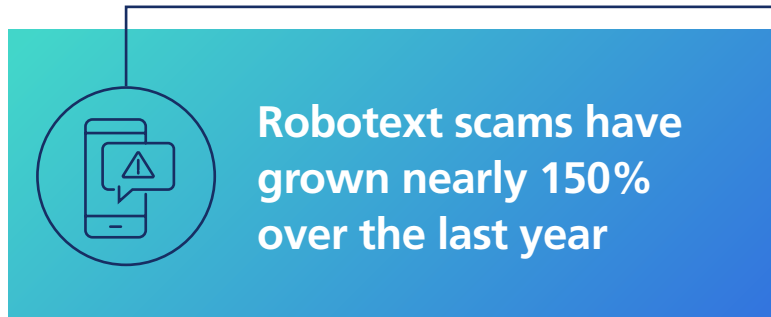
<sup>20</sup><https://www.consumer.ftc.gov/articles/before-giving-to-charity>

TNS believes that the number of robotexts have increased due to the following factors:

- **Bad actors adapt tactics.** Scammers and robocallers are constantly evolving tactics to evade oversight, technology and restrictions. As STIR/SHAKEN improves call authentication across carrier networks, robotexts become a logical way around that standard.
- **10 Digit Long Codes (10DLC).** 10DLCs provide each business or organization with its own dedicated number. At just a few dollars per month and the ability to send high volumes of numbers, these commercial long codes are the perfect solution to the message volume and accountability issues. Carriers are still working on developing 10-digit long code products that are harder for carriers and filter/blocking systems to determine text originator authenticity – if it is a human or application generating the text. Until the carriers have 10DLC products for which something like call authentication technology can be applied, spammers can launch text campaigns from large batches of numbers, and then move to the next batch before getting caught.
- **Other factors that will impact robotexts.** Neighbor Spoofing occurs when the bad actors' area code and digits match or closely match the area code and digits of the consumers' number. Likewise, 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. Snowshoe spamming delivers its volume over a wide swath of telephone numbers to remain undetected. Similarly, this same technique that has been observed with robocalls.

The end-users of TNS services provide direct feedback on robotexting through their mobile devices. Top complaints are:

1. Scam/#scam
2. Spam
3. #phishing/phishing
4. stop
5. unsolicited



In addition, TNS found that in December 2021, 48% of the robotext scams were from a robocall spammer. This was gleaned from crowd-sourced feedback.

TNS catalogs the top robotext scams and publishes them on its [website](#).

**Car insurance smishing scam—**Car insurance scams have been a long time robocall scheme that is now common in SMS messaging. These scams are attempting to sell a car insurance bundle that is unbelievably cheap and ultimately a fraud, or they are after personal information including social security, credit card number, and bank account information.

**Fake package scam—**These scams are sent through text message and includes a shortened link to a suspicious website that will ask you to pay the shipping on the package and try to sell you extra services included with a 14-day free trial. Sometimes the messenger may claim to be a major carrier such as Amazon, FedEx, USPS, or UPS, to gain credibility.

**Free prize scam—**These scams are based on common phone or email scams. However, the scammer is not trying to have a text conversation, but rather wants to convince you to click a link by using a topical current event that seems reasonable or enticing you with a free prize. Like robocalls, these scams are trying to obtain your personal information.



## Political Robocalls & Robotexts

In a recent study conducted in December, 2021, TNS found that Americans are fed up with political robocalls and robotexts. While political campaigns and causes rely on robocalls and robotexts to get out the vote and fundraise, Americans have little appetite to receive them ahead of the 2022 midterm elections.

- Only three-in-10 of those surveyed don't mind receiving legitimate political robotexts, while 42% don't mind receiving legitimate political robocalls.
- 79% of consumers believe all political robotexts and robocalls should be banned until there is a better way to filter those that are legitimate from those that are nuisance/scam.
- 56% of Americans believe they have received a political robotext with misinformation over the past 12 months.
- Only 37% of consumers feel it is easy to opt-out of political robotexts, like the 38% who feel it is easy to opt-out of political robocalls.

The survey also revealed a massive gender disparity in attitudes towards robocalls and robotexts. Far more women than men don't want, trust or engage with robocalls and robotexts.

- Only 21% of females do not mind receiving robotexts from legitimate political campaigns and causes, compared to 40% of men who don't mind receiving them.
- A mere 19% of females do not mind receiving robocalls from legitimate political campaigns and causes, compared to 42% of men who don't mind receiving them.
- Only 19% of women (compared to 38% of men) trust the content of robotexts more than they trust content and source of robocalls.

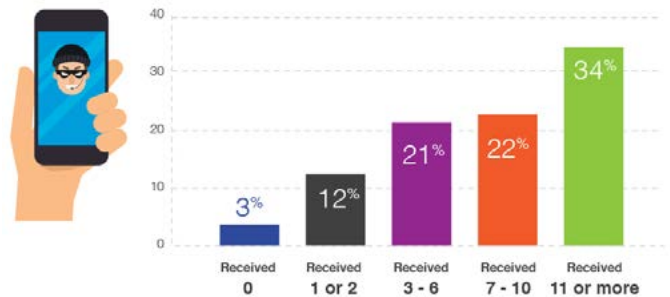
## Senior Scams

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>21</sup>

Additional findings from the survey:

- **Robocall volume is high among seniors.** Almost 90% (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 in early 2021 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. A majority of respondents (63%) 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. 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 the 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.

<sup>21</sup><https://tnsi.com/robocallers-tried-to-scam-nearly-half-of-senior-citizens-out-of-money-in-2019/>



- **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: the federal government (20%); my wireless/wireline carrier (18%); businesses trying to sell me products/services (9%); robocall blocking mobile app vendors (6%); my state government (5%); while 35% said all the above are responsible.

## Neighbor Spoofing

As mentioned earlier, Neighbor Spoofing is a tactic bad actors use to trick consumers into answering their spam calls. 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 numbers will have the same area code or local calling area to incite the consumer to answer. TNS has discovered such patterns and has proactively classified them as medium-risk.

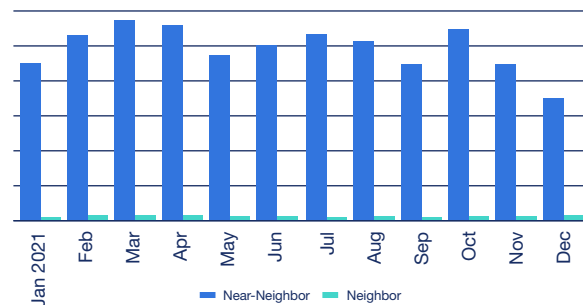
TNS has seen a small decline (~3%) in true neighbor spoofing, as bad actors are using neighbor spoofing less due to implementation of STIR/SHAKEN on the major wireless networks. Instead, they have shifted to near-neighbor spoofing where the area codes are the same, but not the first five or six digits. TNS has seen a remarkable increase of 64% 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 3,000 times the volume compared to “pure” neighbor spoofing where the area code and exchange are the same.

## Neighbor Spoofing vs. Near-Neighbor Spoofing—2021



**Near-neighbor spoofing continues to increase at over 60%**

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.





The crowd-sourced feedback in the last section shows that auto warranty spamming continues to be a problem. TNS observed in the 1H2021 Robocall Investigation Report, Seventh Edition that small VoIP providers were purchasing large numbers of sequential telephone numbers and used snowshoe spamming to place a small amount of calls over hundreds of thousands of local telephone numbers. Unfortunately, STIR/SHAKEN isn't the silver bullet to solving this problem.

The analysis from honeypot data available to TNS shows this to be a continuing problem, however, there has been a shift in tactics used by the bad actors. First, low-volume spamming has moved to ultra-low volume spamming using legitimate telephone numbers. In addition, this ultra-low volume spamming is now using spoofing of wireline residential landline telephone numbers. TNS believes this is due to the initial focus of STIR/SHAKEN on the wireless networks and lower penetration of STIR/SHAKEN in the wireline residential market. Implementation of STIR/SHAKEN in these networks might help reduce the techniques that are used by the bad actors.

## Low-volume spamming techniques have grown more sophisticated

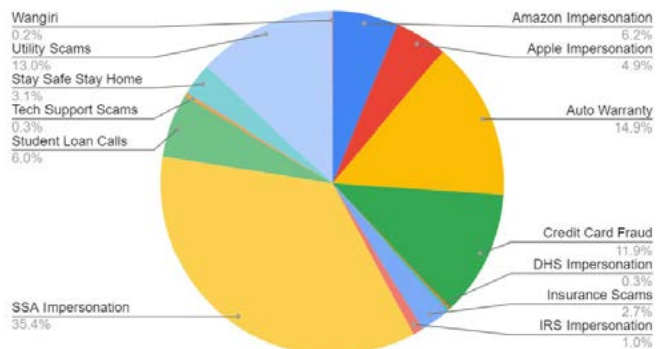


## Report to Congress on Robocalls and Transmission of Misleading or Inaccurate Caller Identification Information

The Enforcement Bureau, Consumer and Governmental Affairs Bureau, and Wireline Competition Bureau filed a report pursuant to Sections 3, 11, and 13 of the *Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act)* that was sent to Congress.<sup>22</sup> Section 3 of the TRACED Act amended the *Telephone Consumer Protection Act (TCPA)* and the *Truth in Caller ID Act* in several respects. The report provided the information that section 3 requires, including data regarding informal consumer complaints that the Commission received during the preceding five full calendar years (2016-2020), and Commission enforcement actions during the preceding calendar year (2020). For this, TNS provided additional informal consumer complaint data and information about Commission enforcement actions through November 30, 2021.

Since January 2021, the **International Traceback Group (ITG)**, USTelecom, has initiated nearly 2,900 tracebacks, representing hundreds of millions of illegal robocalls. Campaigns traced back range from impersonations of government agencies to tech support scams, loan or credit card scams, threats to disconnect utility services and impersonations of brands to sell a product or service, among many others.<sup>23</sup>

Active Campaigns 2021

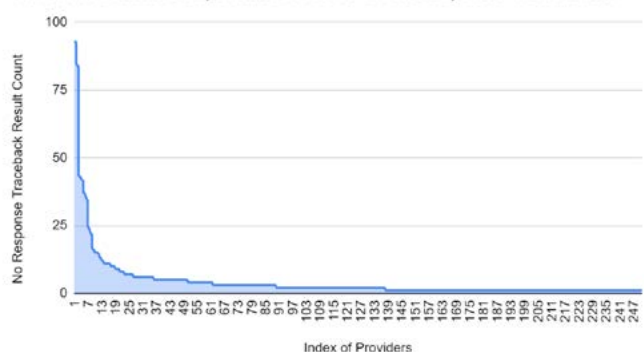


In 2021, nearly 400 domestic and foreign voice service providers have participated in tracebacks so far. Tracebacks have identified 121 U.S. providers originating illegal robocalls, 111 that have brought the calls into the country, and 115 foreign providers originating the illegal traffic. Although some domestic and foreign providers still do not cooperate, as the chart below demonstrates, a handful of non-cooperating providers disproportionately show up in tracebacks.



## 10% of providers responsible for 55% of no response tracebacks

10% of Providers Responsible for 55% of No Response Tracebacks



<sup>22</sup><https://www.fcc.gov/document/fcc-submits-traced-act-annual-report-2021-congress>

<sup>23</sup><https://www.fcc.gov/document/fcc-submits-traced-act-annual-report-2021-congress/attachment-b>

## STIR/SHAKEN Attested Traffic

While STIR/SHAKEN cannot address an incoming call's intent, it does authenticate the calling number and 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.

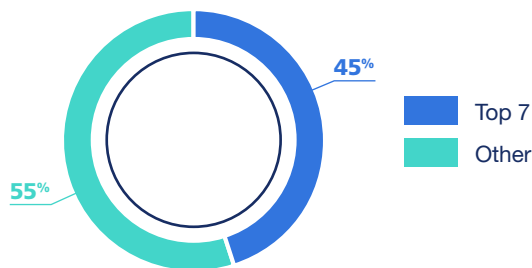
However, the amount of cross-carrier traffic between the seven largest US carriers (AT&T, CenturyLink, Charter, Comcast, T-Mobile, US Cellular and Verizon) account for less than half of the volume.

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

### Cross-Carrier Traffic Among Tier-1 Carriers—2021

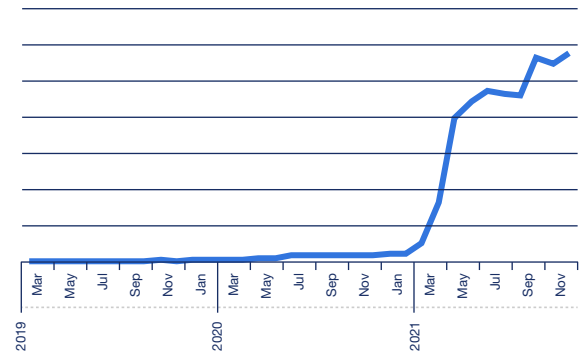


**Partial Attestation (B)**—The service provider has authenticated the call origination, but cannot verify the call source is authorized to use the calling number

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

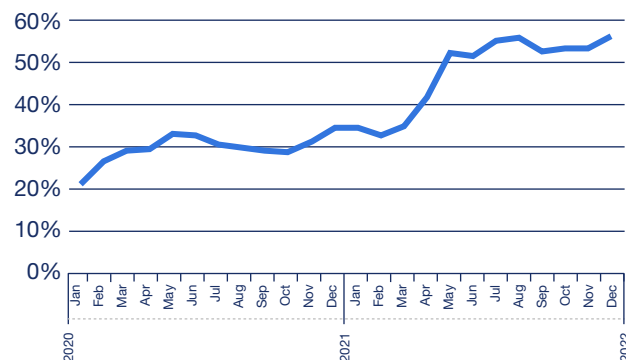
The amount of inter-carrier traffic that TNS has seen shows attestation has continued to grow dramatically in 1H2021.

### 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 56% by the end of 2021.

### STIR/SHAKEN Traffic to Total Traffic



The increase is encouraging but needs to be more widely adopted before it can have a significant impact. In addition, TNS found issues with the early implementations of STIR/SHAKEN. For example, TNS has observed A-level attestation on telephone numbers that are malformed, invalid or on a DNO list. In addition, TNS has seen where telephone number validation has failed. This might very well be a spoofing event or might just be a poor implementation of the STIR/SHAKEN standards.

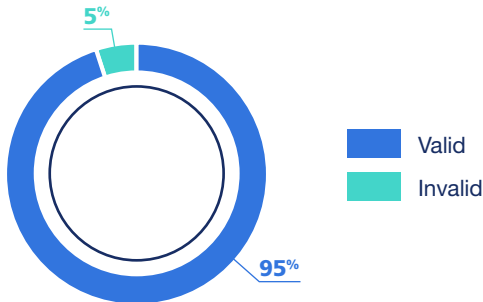
**STIR/SHAKEN**  
needs to expand  
beyond the Tier-1  
providers to have a  
significant impact



## 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 over 50% comparing 2021 to 2020. 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—2021



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.

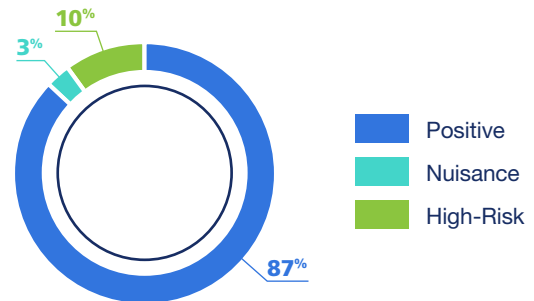
## Canadian Results

Last 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.

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

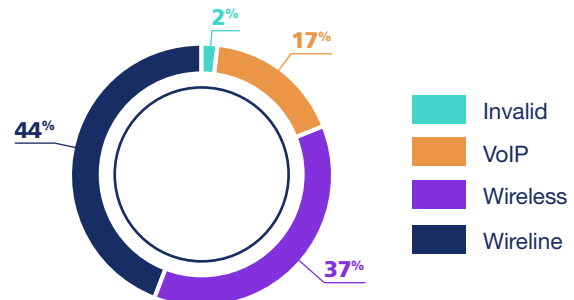
TNS found less than 20% of Canadian inter-carrier calls in 2021 were scored as unwanted, consistent with 2020 and 2019.

### Scoring by Category Canadian Telephone Numbers—2021



Wireline 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—2021



## International Results

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

The 2021 data shows 75% of calls from an international number as positive, and significantly lower than the first half of the year at 84%.

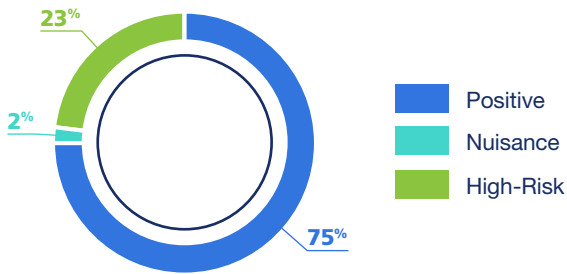
Many of the high-risk calls that come from international numbers are associated with **Wangiri** attacks.

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.

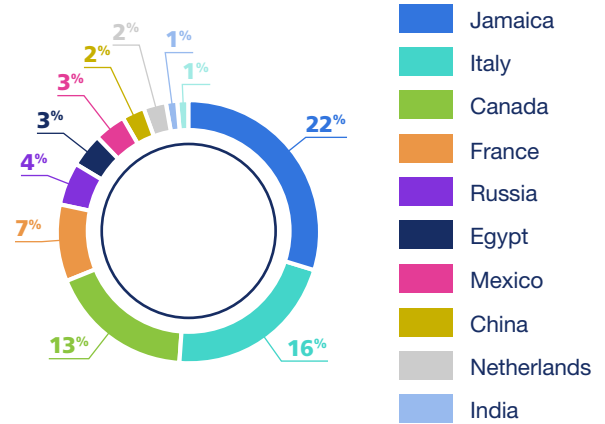
Every time you call, you will be charged high international rates or other connection fees. The bad actor profits from those fees.

### Scoring by Category International Telephone Numbers—2021



The top countries that have unwanted calls coming from their numbering resources are summarized to the right.

### Unwanted Calls from International Telephone Numbers—2021



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



# How Carriers Should Address FCC Rule on Automatic Call Blocking

**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 All 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>24</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

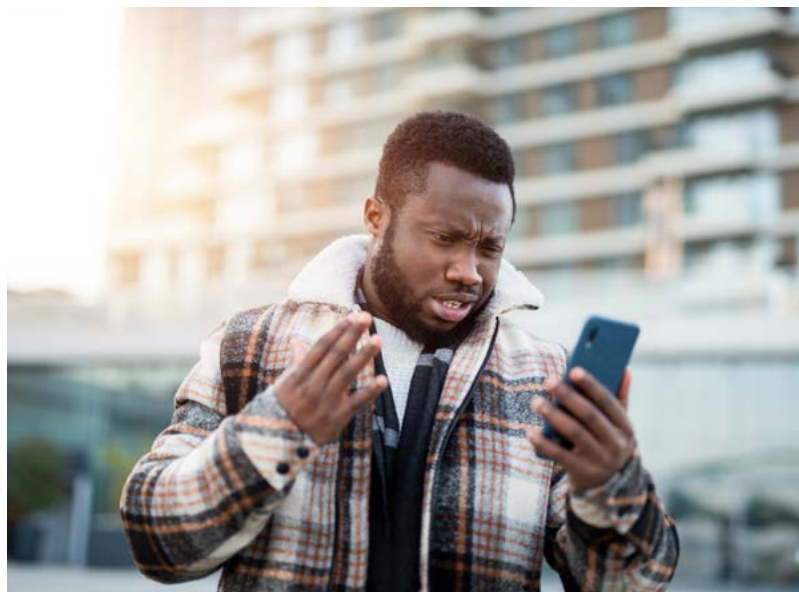
Without trust in the underlying data, it is impossible for consumers to feel comfortable in ceding control in call blocking. Today, it is already possible to detect caller ID spoofing and other malicious and nuisance robocalling behavior based on real-time network data analytics.

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 1.5 billion calls per day across more than 500 telecom operators enable it to identify robocall tactics and trends and confirm which calls are legitimate; machine learning then provides intelligence that can be applied to that 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.



<sup>24</sup><https://tnsi.com/tns-robocall-survey-consumers-want-more-control-or-options-to-combat-robocalls/>



## 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>25</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.

## Branded Calling When it Comes to 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.

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.

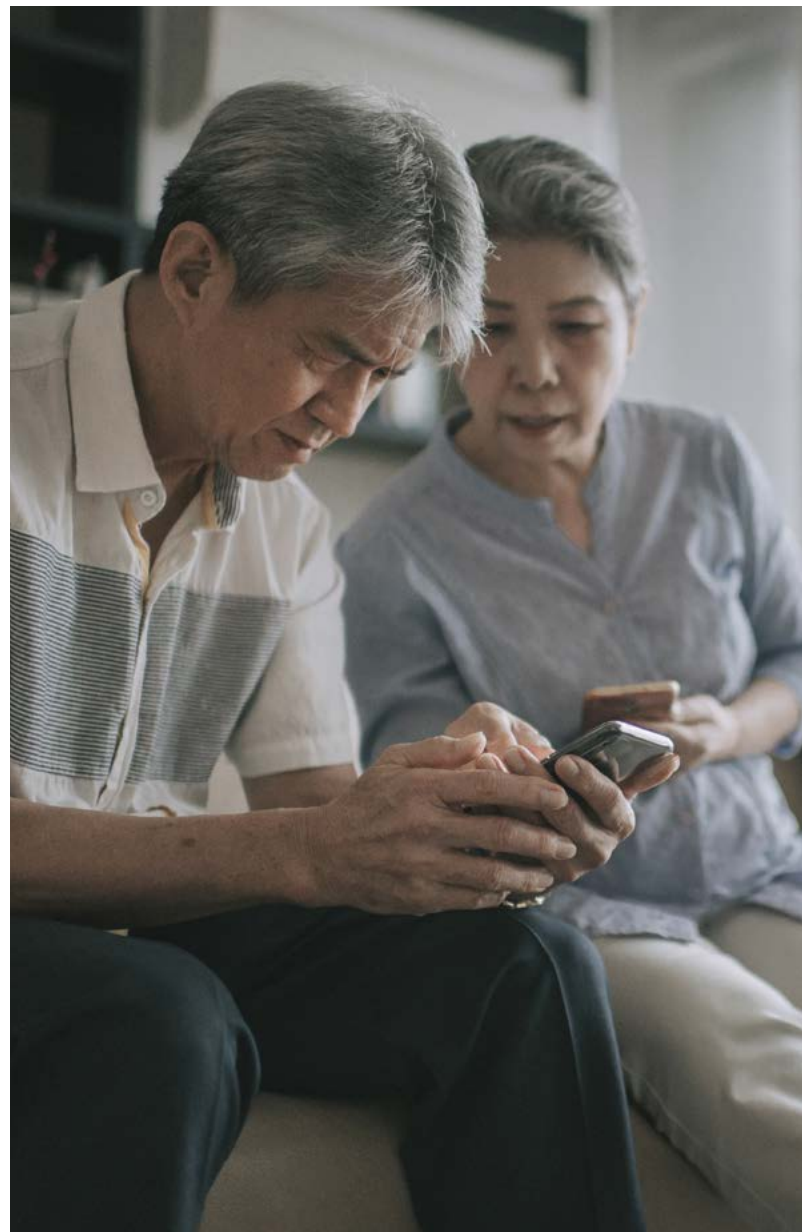
The point is that building consumer confidence in a validation system, whether it's secure/unsecure websites or validated/unvalidated incoming calls, is a long process.

Conversely, businesses have full flexibility to use branded calling to deliver their name, logo, and if desired, the intent of the call.

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>25</sup><https://tnsi.com/tns-robocall-survey-consumers-want-more-control-or-options-to-combat-robocalls/>



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

## 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

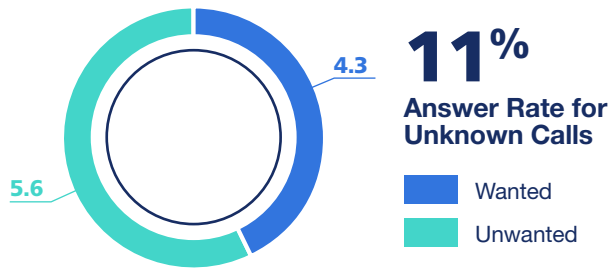
TNS conducted a study in 2021 to understand the trust and behavior associated with incoming calls from enterprises. The goal was to determine how users react when no information is available about a caller. The study provided a baseline of user sentiment of enterprise calls and user expectations of a 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%.



**Call verification is still misunderstood**

### Unknown Calls



Brand presence has strong effect on the consumer trust. A majority of consumers (52%) 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.

The content delivered to the consumer influences trust.

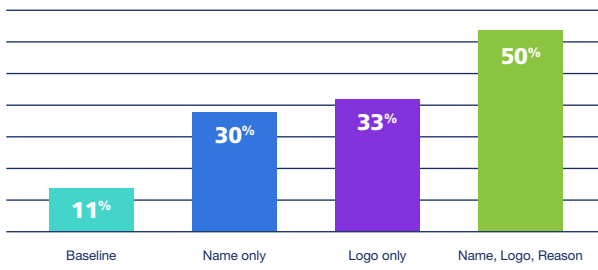
Consumers are five times more likely to answer a call with brand presence than a simple phone number.

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.

### Consumers Most Interested in Calls From

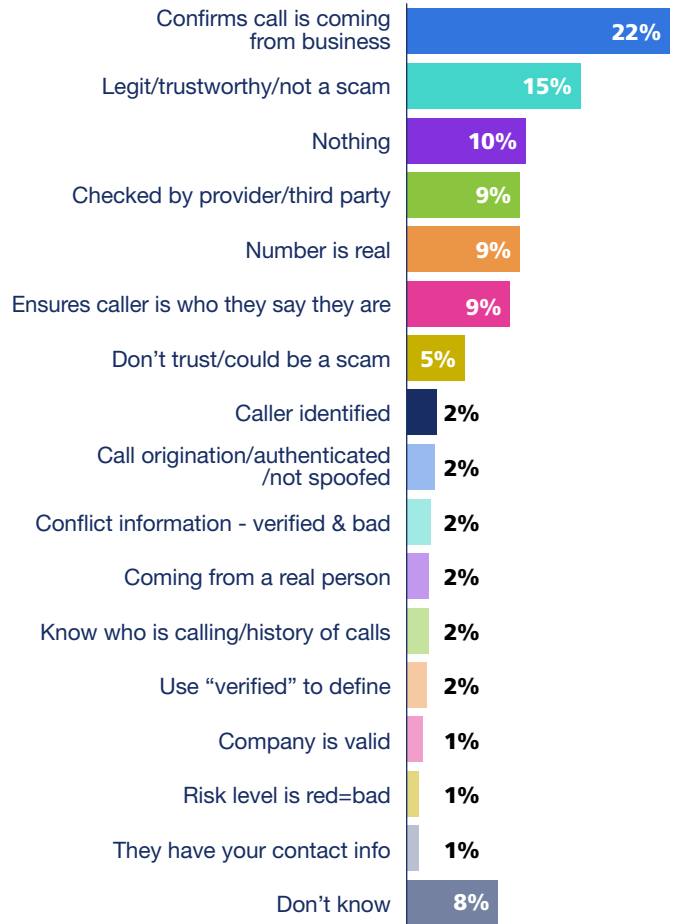


### Percent Likely to Answer



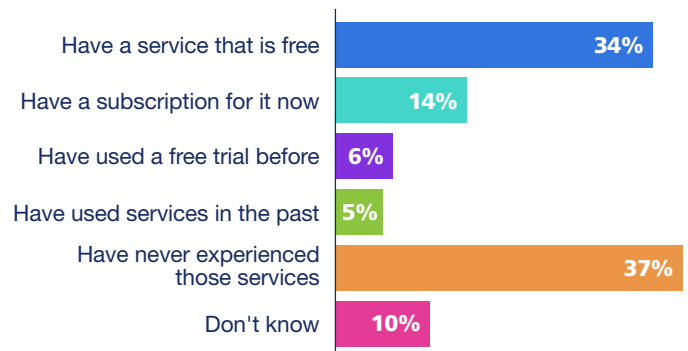
Only 2% understood “caller verified” to mean the number was authenticated and not spoofed. The term meant “nothing” to 10% of consumers. There was also some confusion related to the presence of a risk level which was interpreted as negative and a potential scam risk.

### Interpretations of “Caller Verified” Verstat



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

### Experience with Caller ID/Caller Protection Services



## In the second half of 2021, the FCC focused on continuing the implementation of the TRACED Act and STIR/SHAKEN.

You can refer to the [1H2021 Robocall Investigation Report, Seventh Edition](#) for the actions taken in the first half of 2021.

### FCC Releases Draft Version on Numbering Policy for Modern Communications

In mid-July, the FCC proposed a Notice of Proposed Rulemaking (NPRM) of revisions to rules to better ensure that VoIP providers that obtained the benefit of direct access to numbers comply with existing legal obligations and do not facilitate illegal robocalls, pose national security risks, or evade or abuse intercarrier compensation requirements.<sup>26</sup>

The **NPRM** would do the following:

- Propose to require additional certifications as part of the direct access application process regarding, among other things, compliance with anti-robocalling obligations, and clarify existing requirements
- Propose to clarify that applicants for direct access authorization must disclose foreign ownership information and propose to direct staff to generally refer applications with 10% or greater foreign ownership to the Executive Branch agencies for their views, consistent with the referral of other types of applications
- Propose to clarify that holders of an FCC direct access authorization must update the FCC and applicable states within 30 days of any change to the ownership information submitted to the FCC
- Propose to clarify that FCC staff retains the authority to determine when to accept filings as complete and propose to delegate authority to FCC staff to reject an application if an applicant has engaged in behavior contrary to the public interest or has been found to originate or transmit illegal robocalls
- Seek comment on whether to expand the direct access to numbers authorization process to one-way VoIP providers or other entities that use numbers

### FCC Releases Third Notice of Proposed Rulemaking Call Authentication Trust Anchor; Appeals of the STIR/SHAKEN Governance Authority Token Revocation Decisions Third Report and Order (WC Docket Nos. 17-97, 21-291)

Also, on July 15, 2021, the FCC in the Third Report and Order established a process for voice service providers to appeal such revocation decisions to the FCC.<sup>27</sup>

#### The Third Report and Order:

- Established a process for the FCC to review revocation decisions by the private STIR/SHAKEN Governance Authority, modeled on its established appeals process for reviewing decisions by the Universal Service Administrative Company
- Allows voice service providers aggrieved by a Governance Authority revocation decision to file a request for review to the FCC after completing the Governance Authority appeal process and permit third parties to file oppositions and replies

### FCC Adopted Two Robocall Items in their Open Meeting

On August 5, 2021, the FCC adopted the **Further Notice of Proposed Rulemaking** to adjust the conditions under which interconnected VoIP providers can get **direct access to numbering resources**. The FCC's proposal requires applicants to submit information about foreign ownership and seeks comment on any changes the FCC should make to address access stimulation.<sup>28</sup>

Secondly, the FCC adopted Report and Order establishing a formal FCC review process for any providers that have had their **tokens revoked by the private STIR/SHAKEN Governance Authority**.<sup>29</sup>

### FCC Propose \$5 Million Robocalling Fine Against Jacob Wohl and John Burkman

In the first case under the TRACED Act's TCPA Revisions, the above parties apparently made unlawful robocalls to voters' wireless phones without prior consent. This is the largest TCPA robocall fine ever proposed by the Commission which was done on August 24, 2021. It is also the first action where the FCC was not required to warn robocallers before robocall violations could be counted toward a proposed fine, per Congress's recent amendment of the TCPA.<sup>30</sup>

<sup>26</sup><https://docs.fcc.gov/public/attachments/DOC-374109A1.pdf>

<sup>27</sup><https://docs.fcc.gov/public/attachments/DOC-374110A1.pdf>

<sup>28</sup><https://www.fcc.gov/document/fcc-proposes-updating-numbering-rules-fight-robocalls>

<sup>29</sup><https://www.fcc.gov/document/fcc-establishes-stirshaken-token-revocation-appeals-process-0>

<sup>30</sup><https://www.fcc.gov/document/fcc-proposes-largest-robocalling-fine-under-tcpa>



## FCC Re-ups Industry Traceback Group as Official Robocall Fighting Consortium

On the following day, the Enforcement Bureau within the FCC retained the **USTelecom's Industry Traceback Group**, the incumbent, to continue as the registered consortium that conducts private-led efforts to trace back the origin of suspected unlawful robocalls.<sup>29</sup>

## Wireless Competition Bureau Seeks Comment on Two TRACED Act Obligations

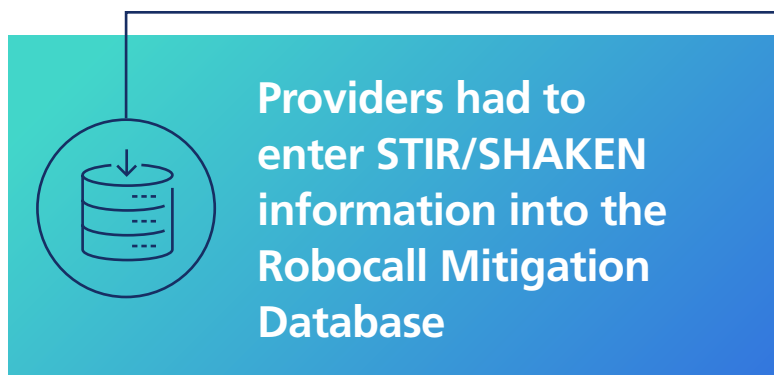
On September 3, 2021, the Wireless Competition Bureau (**WCB**) sought comment on STIR/SHAKEN implementation extensions granted by the Commission. In addition, the Bureau provided directions and filing instructions for the implementation verification certifications that voice service providers granted an exemption from the Commission's caller ID authentication rule must file.<sup>30</sup>

## FCC Issues Notice of Proposed Rulemaking on Shielding 911 Call Centers from Robocalls

On September 9, 2021, the FCC issued an **NPRM** for 911 call centers.<sup>31</sup>

The NPRM would:

- Propose that voice service providers be required to block autodialed calls made to Public Safety Access Point (PSAP) telephone numbers registered on the PSAP Do-Not-Call registry
- Seek comment on the extent to which autodialed calls and text messages continue to be a problem for PSAPs, including whether the number of such unwanted calls has significantly changed in response to technological evolutions since 2012
- Seek comment on the seriousness of the security risks associated with housing registered PSAP telephone numbers in a centralized database and granting access to those numbers to callers purporting to need them to comply with our rules
- Seek comment on whether and how to develop stronger security controls for a PSAP Do-Not-Call registry as well as on whether there are new technological controls that could effectively prevent autodialed calls to PSAP numbers that should be considered
- Seek comment more broadly on ways to protect PSAPs from cyberattacks and disruptions other than those conducted with robocalls



## FCC Announces That Calls from Providers Not Listed in Robocall Mitigation Database Must Now Be Blocked from Domestic Phone Networks

Beginning September 28, 2021, **terminating voice service providers and intermediate providers may not accept calls directly from an originating voice service provider not listed in the Robocall Mitigation Database.** To ease compliance with this obligation, the Bureau also announced the availability of an email subscription service to notify subscribers of additions, deletions, and revisions to filings in the Robocall Mitigation Database.<sup>32</sup>

## FCC Adopts PSAP and Gateway Provider Robocall NPRMs

On October 1, 2021, the FCC proposed to require gateway providers to apply STIR/SHAKEN caller ID authentication to, and perform robocall mitigation on, **foreign-originated calls with US numbers.** This proposal would subject foreign-originated calls, once they enter the United States, to requirements like those of domestic-originated calls, by placing additional obligations on gateway providers considering the large number of illegal robocalls that originate abroad and the risk such calls present to Americans. The FCC further proposed and sought comment on several additional robocall mitigation requirements to ensure that gateway providers take steps to prevent illegal calls from entering the US network.<sup>33</sup>

In addition, the FCC proposed that voice service providers be required to block autodialed calls made to PSAP telephone numbers registered on the PSAP Do-Not-Call registry. The FCC sought comment on this approach and on ways that it can protect PSAPs from attacks and disruption other than those conducted with robocalls.<sup>34</sup>

<sup>29</sup><https://www.fcc.gov/document/fcc-retains-industry-traceback-group-robocall-consortium>

<sup>30</sup><https://www.fcc.gov/document/wcb-seeks-comment-two-traced-act-obligations>

<sup>31</sup><https://www.fcc.gov/document/stopping-illegal-robocalls-entering-american-phone-networks>

<sup>32</sup><https://docs.fcc.gov/public/attachments/DOC-376119A1.pdf>

<sup>33</sup><https://docs.fcc.gov/public/attachments/FCC-21-105A1.pdf>

<sup>34</sup><https://docs.fcc.gov/public/attachments/FCC-21-108A1.pdf>

## Wireline Competition Bureau Adopts Protective Order for Robocall Mitigation Program Descriptions

On October 14, 2021, the FCC released a **Protective Order** that governs the submission of and access to confidential and highly confidential information included in robocall mitigation programs submitted to the Robocall Mitigation Database. Access to filings submitted under the Protective Order is limited to “certain entities and individuals involved in robocall compliance and enforcement.” That list includes: federal, state, local, and Tribal government entities involved in robocall enforcement; the registered traceback consortium; the STI-GA; and intermediate and voice service providers who accept call traffic directly from a provider in the database; but only to such parties’ outside counsel and consultants, as well as the employees and support personnel of these outside firms.<sup>35</sup>

## Acting Chair Rosenworcel Proposes Rules to Combat Rise of Robotexts

On October 28, 2021, the FCC issued an NPRM that requires mobile wireless providers to **block illegal text messaging**, building on the agency’s ongoing work to stop illegal and unwanted robocalls.<sup>36</sup>

## FCC Issues Robocall Cease-and-Desist Letters to Three More Companies

On October 21, 2021, the FCC’s Enforcement Bureau sent cease-and-desist letters to three network providers—**Duratel, Primo Dialler, and PZ/Illum Telecommunication**—demanding that these providers immediately cease originating illegal robocall campaigns on their networks, many of which originated overseas, and report to the Commission the concrete steps they are implementing to prevent a recurrence of these operations.<sup>37</sup>

## FTC Announced an Advanced Notice of Proposed Rulemaking to Combat Government and Business Impersonation Fraud

The FTC staff provided a presentation on December 9, 2021, and the Commission voted on an Advance Notice of Proposed Rulemaking to address rampant government and business impersonation fraud. Government and business impersonation scams are a leading source of consumer complaints and the largest source of total reported consumer financial losses – and have gotten worse during the pandemic.<sup>38</sup>

## FCC Moves Up Small Provider STIR/SHAKEN Start Date to Combat Robocalls

Also, on December 9, 2021, The FCC required *non-facilities-based small voice service providers to implement STIR/SHAKEN a year sooner than previously required*, while maintaining the full extension for those small voice service providers that are facilities-based. The FCC further requires any small voice service providers that the Enforcement Bureau suspects of originating illegal robocalls and that fails to mitigate such traffic upon Bureau notice or otherwise fails to meet its burden under section 64.1200(n)(2) of its rules, to implement STIR/SHAKEN within 90 days of that determination unless sooner implementation is otherwise required.<sup>39</sup>

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

## FCC Released an Order on Reconsideration, Sixth Further Notice of Proposed Rulemaking, and Waiver Order

On December 14, 2021, the **Order on Reconsideration** does the following:

1. Permits terminating voice service providers to utilize SIP Code 603 “during the finalization of and transition to SIP Codes 607 and 608.” Note that the Order does not delay the effective date of the requirement, but rather allows providers to rely on SIP Code 603, or SIP Codes 607 or 608, to comply with the requirement that took effect on January 1, 2022
2. Confirms that notification is only necessary for calls blocked pursuant to an analytics program, and not to, for instance, calls blocked based on a Do-Not-Originate list, in the case of a telephone denial of service attack, or pursuant to customer-initiated blocking (e.g., allow/disallow lists, Do-Not-Disturb, call rejection, and line-level blocking)
3. Clarified that a provider’s blocked call list need only include calls blocked based on opt-in or opt-out analytics-based blocking programs, and does not need to include, for instance, calls blocked based on subscriber-initiated programs or pursuant to network-based blocking
4. Clarifies that originating voice service providers must make the response code available to callers that are able to receive it

<sup>35</sup><https://www.fcc.gov/document/protective-order-adopted-robocall-mitigation-program-descriptions>

<sup>36</sup><https://www.fcc.gov/document/acting-chair-rosenworcel-proposes-rules-combat-rise-robotexts>

<sup>37</sup><https://www.fcc.gov/document/fcc-issues-robocall-cease-and-desist-letters-3-more-companies>

<sup>38</sup>[https://www.ftc.gov/news-events/press-releases/2021/12/ftc-announces-tentative-agenda-december-16-open-commission?utm\\_source=govdelivery](https://www.ftc.gov/news-events/press-releases/2021/12/ftc-announces-tentative-agenda-december-16-open-commission?utm_source=govdelivery)

<sup>39</sup><https://www.fcc.gov/document/fcc-moves-small-provider-stirshaken-start-date-combat-robocalls-0>

<sup>39</sup><https://docs.fcc.gov/public/attachments/DOC-375608A1.pdf>

# Industry Solutions to Combat Robocalling

## Hardware and Software

There are multiple hardware and software solutions available. Many products are limited to using only a single medium, such as traditional copper 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 further 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 which connect to the telephone. 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>40</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, crowd-sourcing 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's database of known genuine numbers, highlighting the danger of centralizing this information.<sup>41 42</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>43</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.

<sup>40</sup><https://www.consumerreports.org/cro/magazine/2015/07/robocall-blocker-review/index.htm>

<sup>41</sup><https://blog.truecaller.com/2013/07/18/truecaller-statement/24>

<sup>42</sup><http://www.ehackingnews.com/2013/07/truecaller-database-hacked-by-syrian.html>

<sup>43</sup>[https://apps.fcc.gov/edocs\\_public/attachmatch/DA-16-1121A1.pdf](https://apps.fcc.gov/edocs_public/attachmatch/DA-16-1121A1.pdf)

In simple terms, each TSP obtains their digital certificate from a certificate authority who is trusted 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 they 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

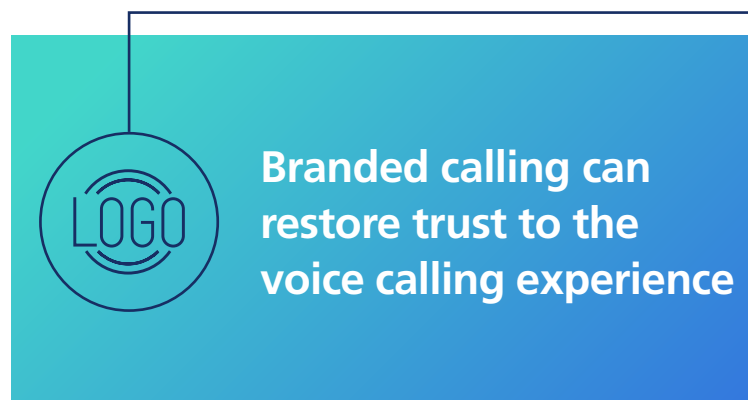
TNS has observed a varied response among enterprises to the mitigation techniques that the industry has employed. Among the good actors, there has been a general willingness to adapt methodologies to conform with the analytics tools' definitions of good behavior.

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

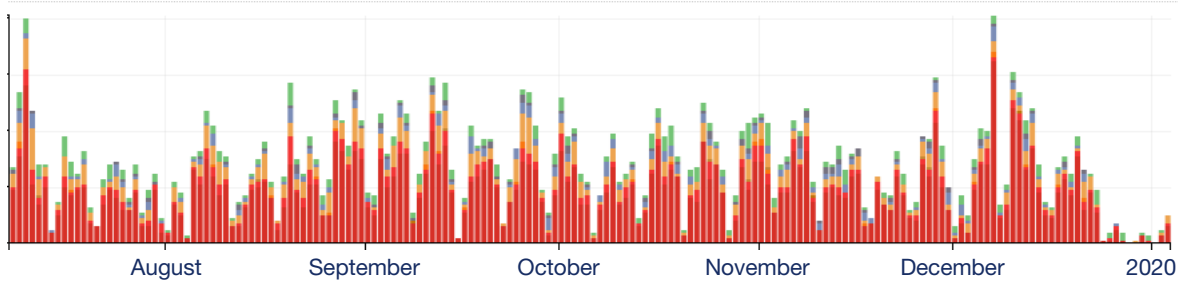
Further, products that provide call origination aggregators and enterprises with a view into their call centers' practices, such as **Telephone Number Reputation Monitoring** from TNS, allow them to understand how their numbers are being characterized, and when activity triggers unwanted reputational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





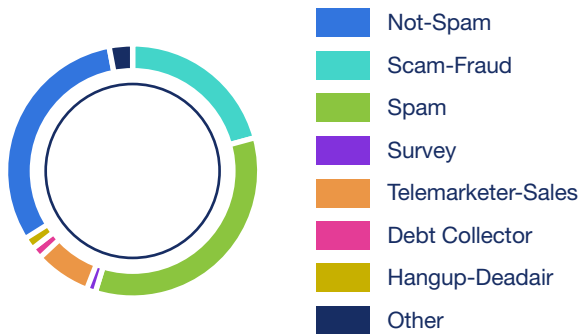


Above is an example showing the mixed customer feedback.

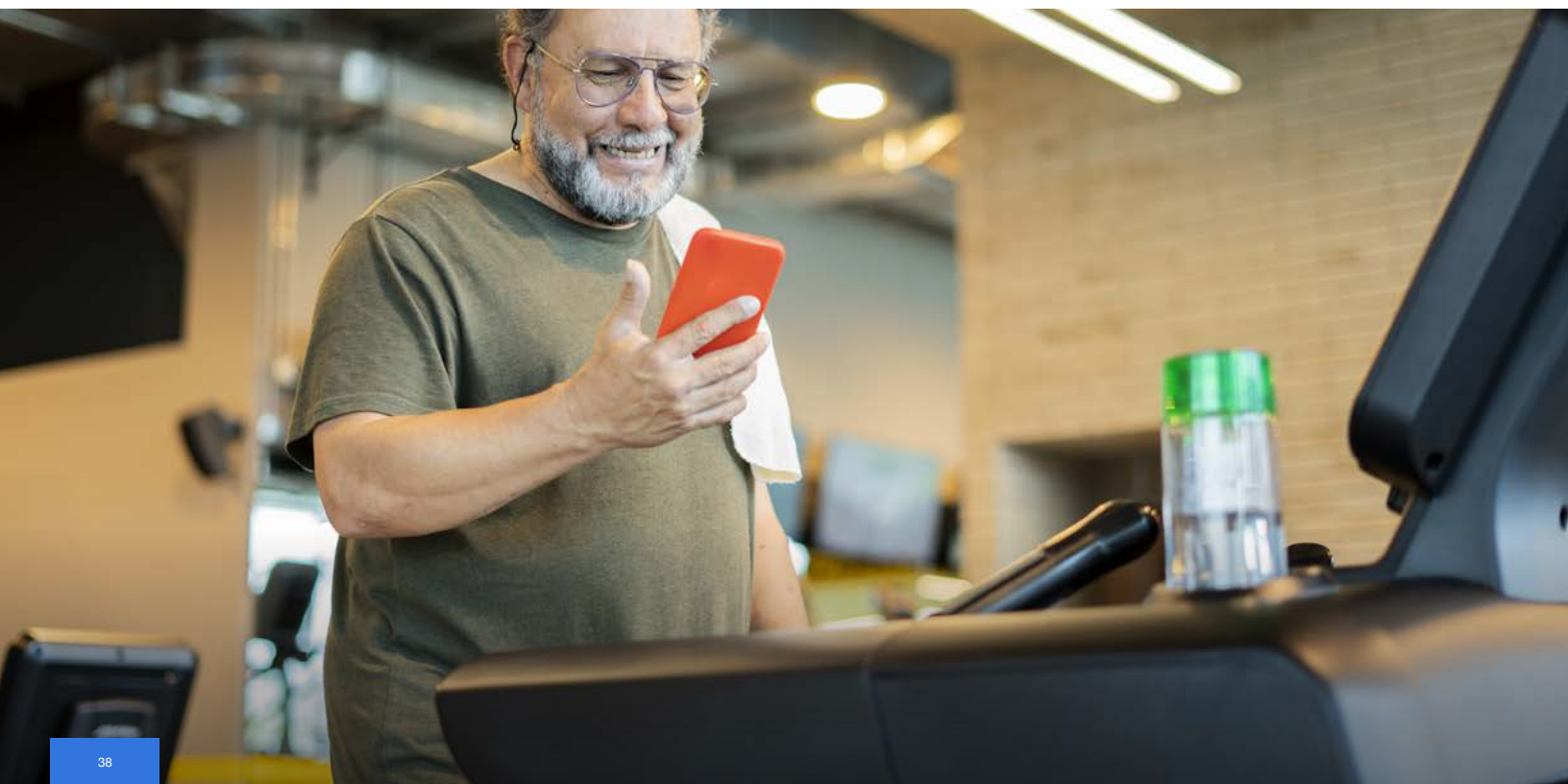
The color of feedback corresponds to the color in the pie chart below, with blue being reports of scam-fraud.

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

#### Category Distribution



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



**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.**

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.

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.

A circular icon containing a stylized graphic of three stacked layers with a downward-pointing arrow above them, representing a layered approach.

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







**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)**

©2022 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