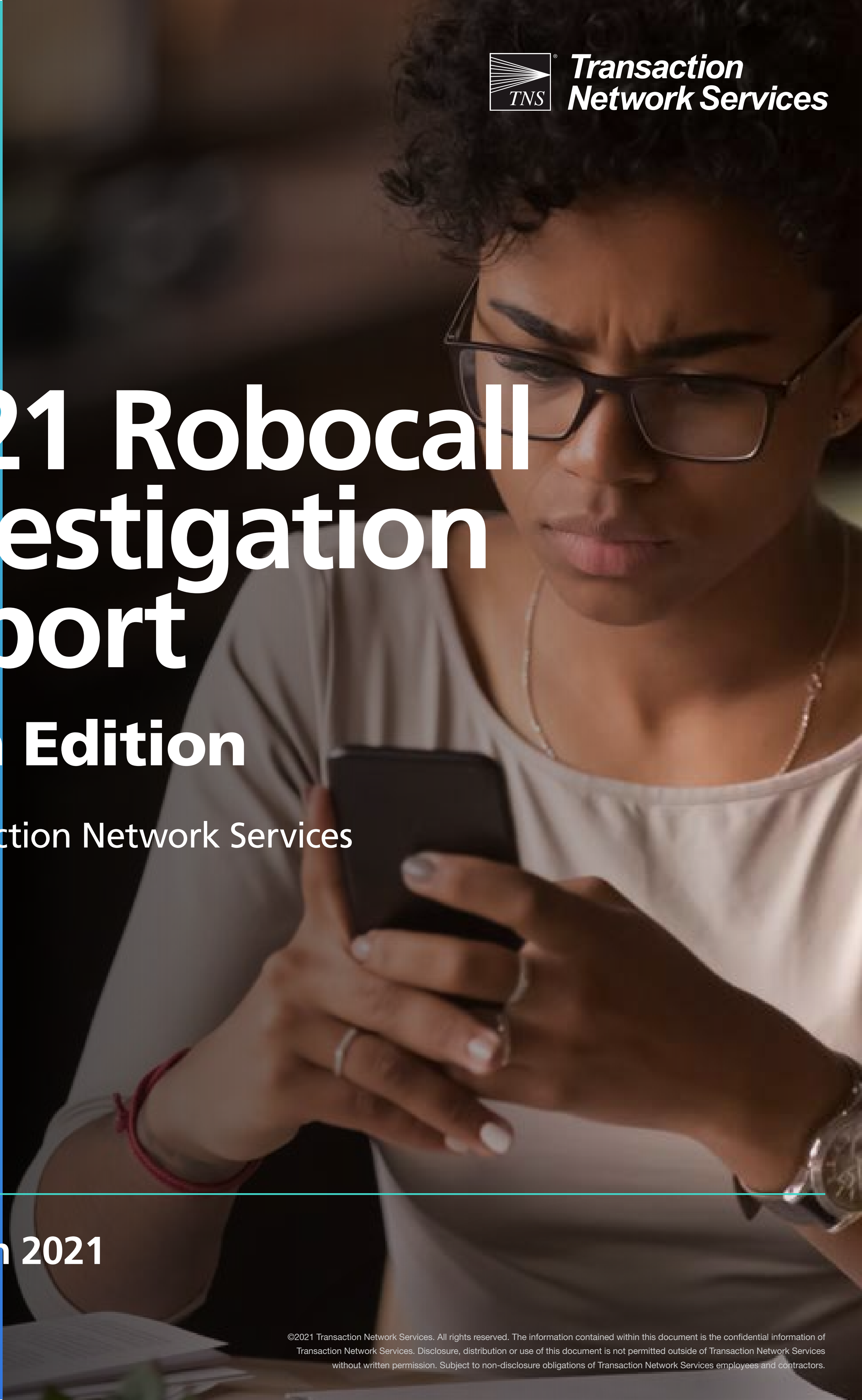


2021 Robocall Investigation Report

Sixth Edition

By Transaction Network Services

March 2021

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
28

Industry Solutions to Combat Robocalling
32

Conclusions and Recommendations
35

Executive Summary

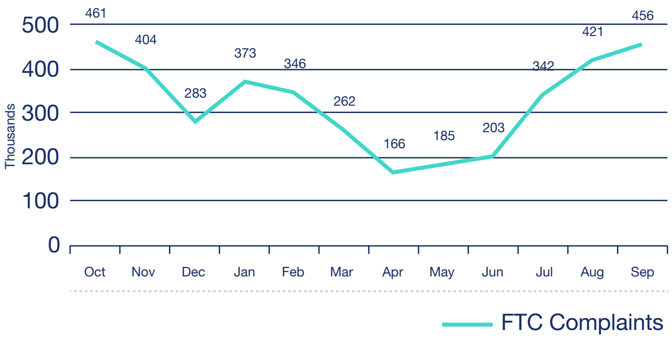
The TNS 2021 Robocall Investigation Report, Sixth Edition (Robocall Report) is a continuing examination into the data, convention and trends that plague consumers' phones daily.

TNS Call Guardian, the industry-leading big-data analytics engine, has gained insights and reputation data on over 1.9 billion phone numbers by analyzing one billion daily call events across hundreds of carriers.

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

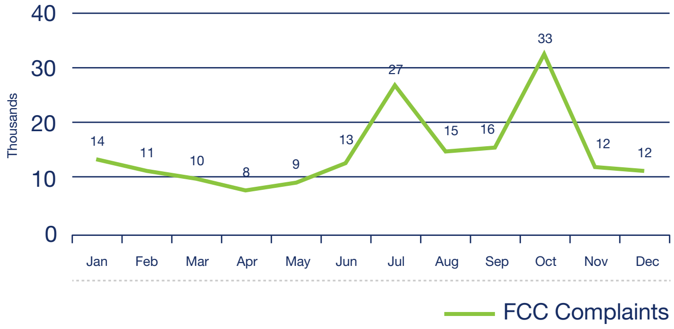
- Robocalling, spamming, scamming, and spoofing declined 28% in unwanted calls in 2020 compared to 2019.
- The Federal Trade Commission (FTC) saw a similar decrease in complaints received, down 31% when comparing January-September of 2020 to the same period in 2019.[1]

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



- In December 2020, the FTC announced that Alcazar and its owner Gavin Grabias assisted and facilitated illegal robocalls in violation of the FTC's Telemarketing Sales Rule (TSR). The FTC imposed a $105,562 judgment against the defendants. This was the second action taken against a voice-over internet protocol (VoIP)[2]
- Imposter scams topped the list of consumer complaints submitted in the last 12 months to the FTC's nationwide Consumer Sentinel followed by reducing debt scams. Medical and prescription scams was the third highest complaint. These top three scams account for 27% of the complaints to the FTC.[3]
- The Federal Communications Commission (FCC) saw a negligible drop in the number of complaints for the Do-Not-Call Registry of 5% when comparing 2020 to 2019, according to their consumer complaint data.[4]

FCC Complaints—Last 12 Months



- Carriers have begun to block some of these calls permissible by the FCC order. Carriers also have made low-cost tools available to their wireless subscribers and have educated them on robocalling.

Imposter Scams

About
1 in 10 People
Lost Money

$667 Million Reported Lost
$700 Median Loss

Identity Theft Reports

88% ↑
Credit Card New Account Fraud

29% ↓
Tax Fraud

Federal Trade Commision • ftc.gov/data

[1] https://public.tableau.com/profile/federal.trade.commission#!/vizhome/DoNotCallComplaints/Maps
[2] https://www.ftc.gov/news-events/press-releases/2020/05/ftc-obtains-final-order-against-do-not-call-violator-bannin-him
[3] https://public.tableau.com/profile/federal.trade.commission#!/vizhome/DoNotCallComplaints/Maps
[4] https://opendata.fcc.gov/Consumer/Consumer-Complaints-Data-Unwanted-Calls/vakf-fz8e

Consumer fatigue and recognition that complaining to the authorities won't have a major impact has led to a reduced number of complaints received by the FTC and FCC. TNS estimates that over 77 billion unwanted calls were placed in the last 12 months.

Over 77 billion unwanted calls in last 12 months

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

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

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

In addition, the report takes a closer look at the impact of **COVID-19 scams** and TNS has expanded the section on top scams to include robocall data on the Democratic primaries, the Presidential election and the Georgia Senate run-off.

What valuable insights can your organization learn?

Here is a summary of findings discussed in this report:

- **Unwanted calls declined for the year.** Unwanted calls dropped 28% in 2020 vs. 2019. Over 77 billion unwanted calls have been made in the last 12 months.
- **Tier-1 carriers continue to be a small part of the problem.** Almost 95% of high-risk calls originate from non-Tier-1 telephone resources, up 3% from last year.
- **STIR/SHAKEN is being adopted by the carriers.** Of the carriers that have deployed (Secure Telephone Identity Revisited) / (Signature-based Handling of Asserted information using toKENs) (STIR/SHAKEN), more than one-third of the total calls in December were self-signed, up from 21% in the beginning of the year.
- **Wireline is twice as bad as wireless.** More than a third of the total calls (37%) to wireline telephone numbers are unwanted compared to 17% for *wireless* telephone numbers. In addition, the trend of unwanted calls to wireline has increased as a percentage of unwanted calls.
- **Spoofing of legitimate enterprise and government entity toll-free numbers continues to increase at a growing rate.** Toll-free originated calls now account for more than one-third (35%) of the high-risk call volume, up from 28% in second half of 2019.
- **Neighbor spoofing continues to decline.** Use of same area code and prefix saw a decrease of 43% on a per subscriber basis from 2019 to 2020, while use of the same metropolitan area codes to call a subscriber (near-neighbor spoofing) has increased 17% in the same period.

Introduction

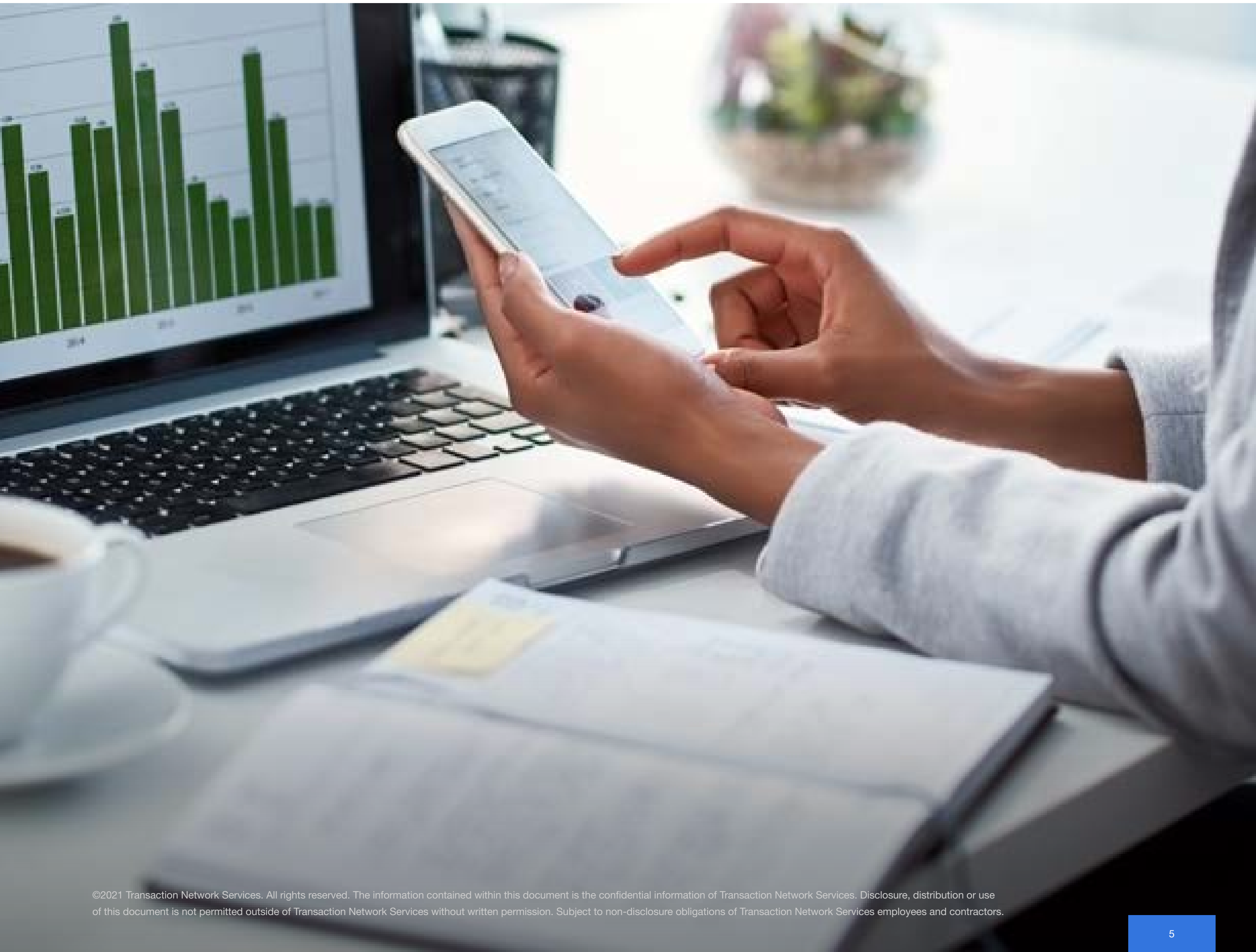
The TNS 2021 Robocall Investigation Report, Sixth Edition includes a vast amount of factual evidence derived from real network traffic over the last three years.

The study is unique in that it offers an objective, first-hand view of robocalling, spamming and spoofing across 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 to access the data and applications they need over managed and secure communications platforms.

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

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



The Telephone Consumer Protection Act 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.[6]

Fraud amounts to about $1.9 billion annually

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.

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.

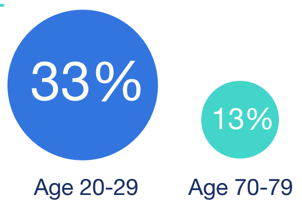
Those illegitimate businesses may not just be annoying consumers, they also may be trying to defraud them.

Consumers lost an estimated $1.9 billion to fraud in 2019 – 28% more than in 2018.[7]

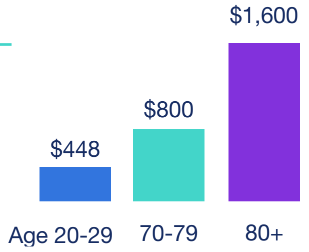
Younger people reported losing money to fraud more often than older people. In 2019, 33% of people in their 20s reported a loss to fraud, while only 13% of people in their 70s.[8]

However, when people in their 70s did lose money, the amount tended to be higher: their median loss was $800, compared to $448 for people in their 20s.[9]

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



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



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

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

As of September 30, 2020, the registry had over 241 million active registrations, an increase of two million registrations from the same time period in 2019.[10]

However, the lists have been ineffective. While legitimate call originators honor the list, illegitimate callers 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.[11]

[6] https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts

[7] https://www.ftc.gov/system/files/documents/reports/national-do-not-call-registry-data-book-fiscal-year-2019/dnc_data_book_2019.pdf

[8] https://www.ftc.gov/system/files/documents/reports/national-do-not-call-registry-data-book-fiscal-year-2019/dnc_data_book_2019.pdf

[9] https://www.ftc.gov/system/files/documents/reports/national-do-not-call-registry-data-book-fiscal-year-2019/dnc_data_book_2019.pdf

[10] https://www.ftc.gov/news-events/press-releases/2019/10/ftc-releases-fy-2019-national-do-not-call-registry-data-book

[11] https://ieeexplore.ieee.org/document/7546510/

Methodology

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

Call Guardian analyzes over one billion daily call events across hundreds of carriers and bases 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 similar to one's own phone number.

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

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

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

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

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

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

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

Layered Approach to Identifying Bad Actors

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

Results and Analysis

Reputation Category and Scoring

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

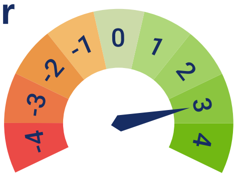
Categories are indicative of legitimate, abusive, fraudulent and unlawful call behavior—inclusive of any call placed via auto-dialer or manually dialed.

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

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

Category
Robocaller

Score
3



Positive Robocalls

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

Examples Include:

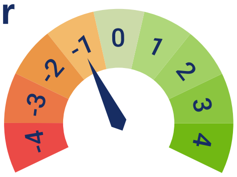
Public service announcement
Calls that are placed to inform a community of an event, such as a school closing.

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.

Category
Robocaller

Score
-1



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:

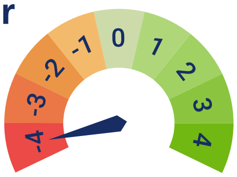
Promotional offers
Calls made to customers who have not given prior explicit consent.

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.

Category
Robocaller

Score
-4



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.

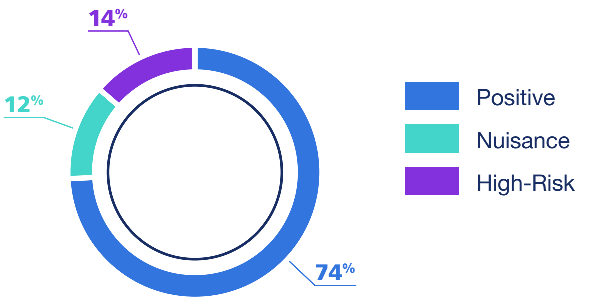
COVID-19 cures
Calls selling fraudulent products that claim to prevent mitigate or detect the coronavirus.

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 27% of the inter-carrier calls in in the first half of 2020 were scored as unwanted, dropping from the rate of 30% that had been consistent from 2017 through 2019.

TNS believes this is due to carriers blocking more calls in the network and the COVID-19 pandemic. Both bad actors and legitimate call originators struggled with the shutdowns and shifting resources to “work from home” (WFH) that occurred in March.

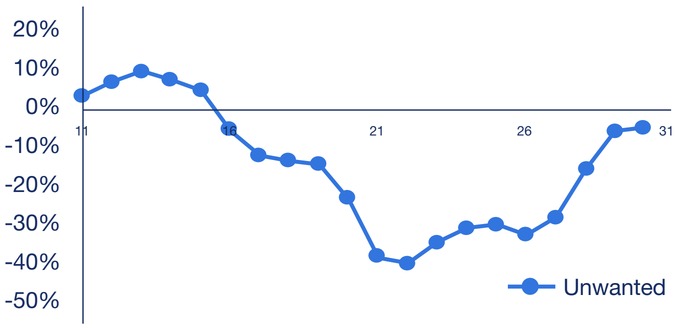
Scoring by Category—2020



TNS saw a drop in both unwanted and wanted calls starting in mid-March. The following chart shows the week-over-week changes in calling activity.

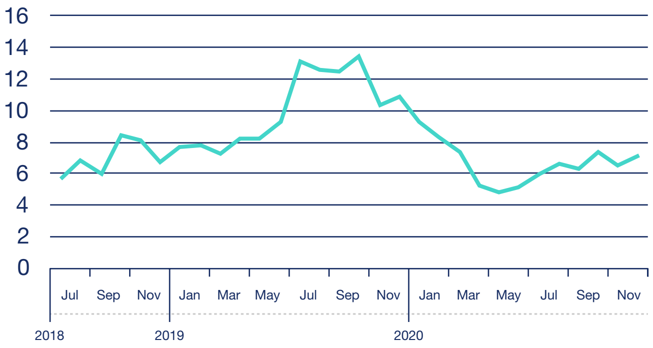
COVID-19 had an impact on unwanted call volume

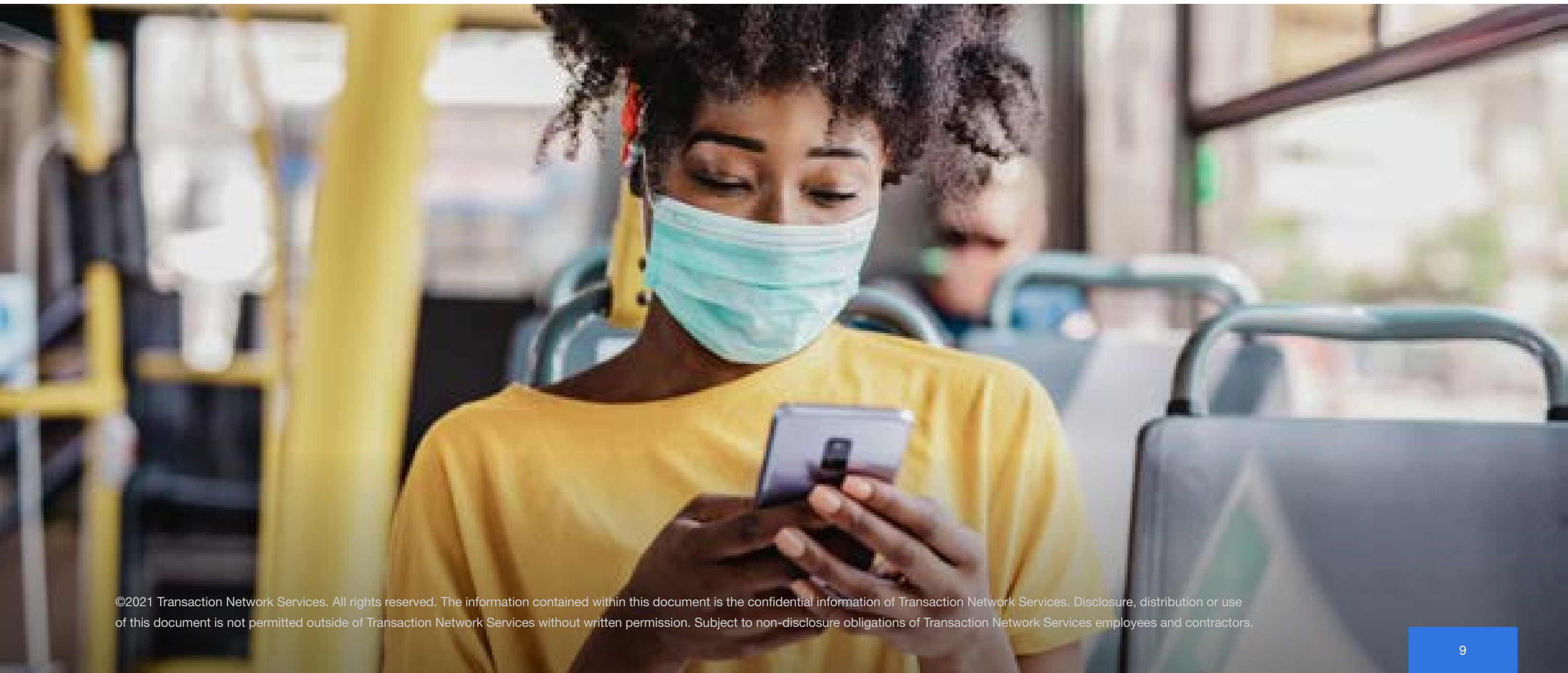
Change in Unwanted Calls—March 2020



As a result of WFH earlier in the year, nuisance calls saw a negligible decrease of 1% from 1H2020 to 2H2020. However, unwanted calls started to show an increase starting in June that continued through November. The election had a significant contribution to the unwanted call volume leading up to November.

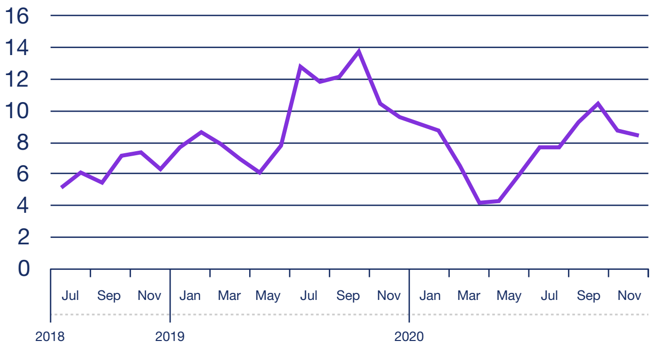
Nuisance Calls per Telephone Number





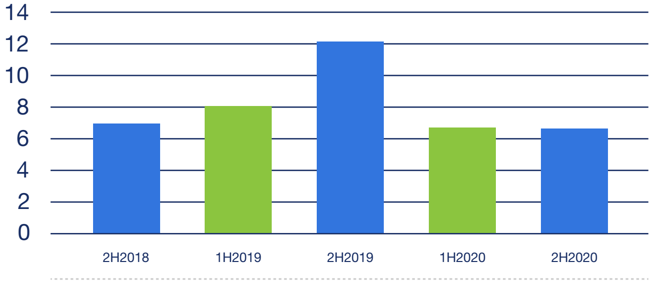
High-risk calls increased 35% from 1H2020 to 2H2020.

High-Risk Calls per Telephone Number

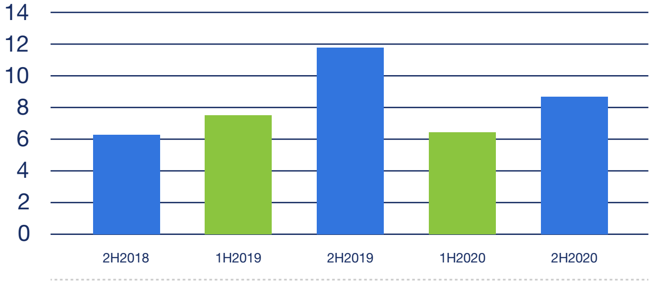


The following charts show the number of nuisance and high-risk call per month by quarter for the last two and half years. Both nuisance and high-risk calls decreased in the second half of the year from the second half of the previous year.

Average Nuisance Calls per Month per Telephone Number



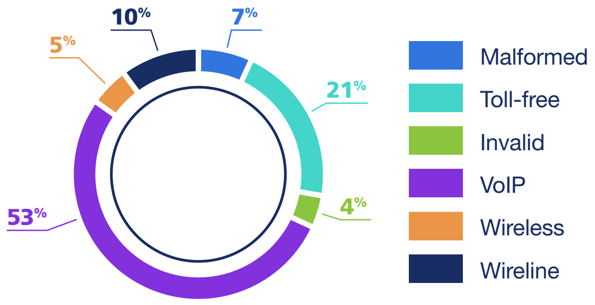
Average High-Risk Calls per Month per Telephone Number



Origination of Unwanted Calls

Not surprisingly, VoIP-originated calls generated more than 50% of the unwanted scored calls in 2020 by total volume, consistent with 2019. Toll-free originated calls represented the second highest amount at 21%.

Distribution of All Unwanted Calls—2020



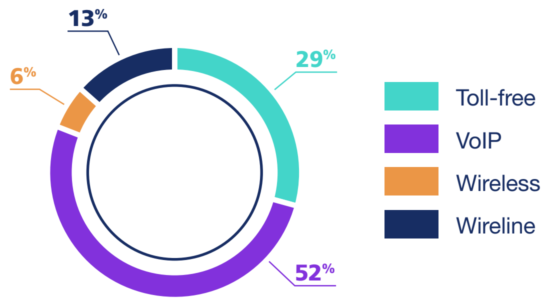
A provider that allows users to bring their own device and unbundles service so that direct inbound numbers may be purchased separately from outbound calling minutes are another source for bad actors.

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

Providers that market "wholesale VoIP" allow any displayed number to be sent, as resellers will want their customer's numbers to appear.[12]

Nuisance calls continue to be led by VoIP telephone numbers and the share of calls coming from VoIP telephone numbers increased from 48% of the calls in 1H2020 to 52% of the calls for *all* of 2020.

Distribution of Nuisance Calls—2020



[12] https://www.fcc.gov/document/fcc-urges-more-phone-industry-join-tracing-scam-robocalls

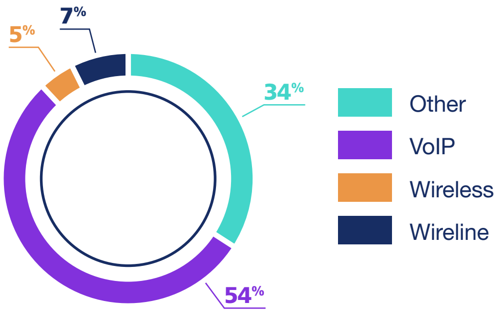
While there are legitimate reasons to modify the calling number, bad actors use this technique to hide their identity.

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.

Toll-free originated calls continue to grow as a larger part of the high-risk calls

VoIP telephone numbers still represent the largest source (54%) of high-risk calls. Invalid and malformed numbers are included in the "Other" category along with toll-free numbers and account for the second highest source of high-risk calls in the chart below.

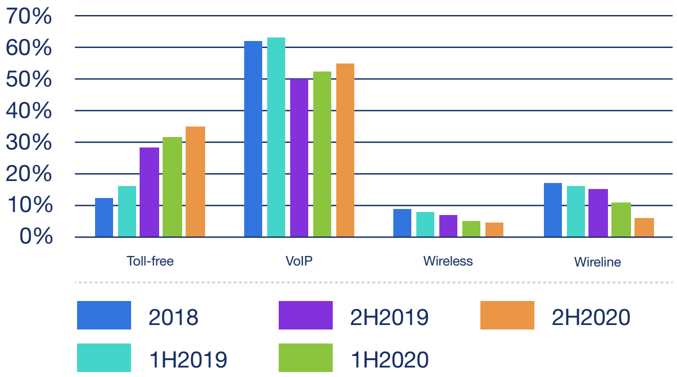
Distribution of High-Risk Calls—2020



Spoofing of wireless telephone numbers for high-risk calls declined from 2H2019 to 1H2020. They have shifted to near-neighbor spoofing where the area codes are the same, but not the first five or six digits which is being done primarily by VoIP numbers.

As indicated in previous Robocall Investigation Reports, bad actors have shifted calling from VoIP telephone numbers to toll-free numbers. Unwanted, high-risk calls from toll-free numbers jumped to 35% last year from 26% in 2019 and 12% in 2018.

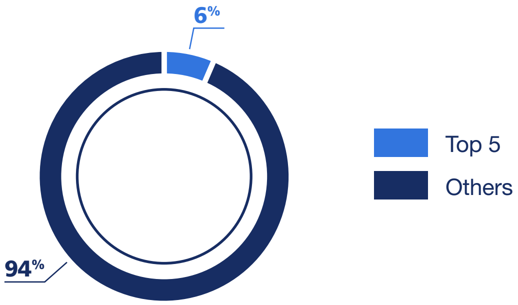
Distribution of High-Risk Calls Over Time



Implementation of **STIR/SHAKEN** framework by AT&T, Comcast, T-Mobile and Verizon has likely resulted in the decrease of VoIP calls that are unwanted.

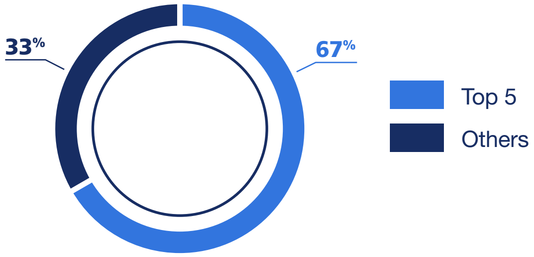
It is important to note that only 6% of the high-risk calls in 2020 originated from the top five carriers (AT&T, CenturyLink, Comcast, T-Mobile and Verizon). This is a significant drop from 11% in 2019.

Telephone Numbers Placing High-Risk Calls



However, when you add in calls from the top six carriers, they still account for 70% of the total number of calls in 2020, up slightly from 68% in 2019.

Telephone Number Resources—Total Calls

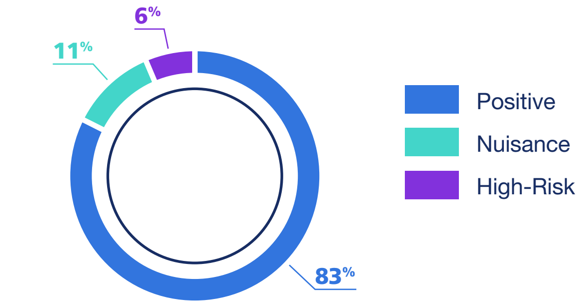


Almost 95% of scam/fraud calls come from numbers not owned by Tier-1 carriers

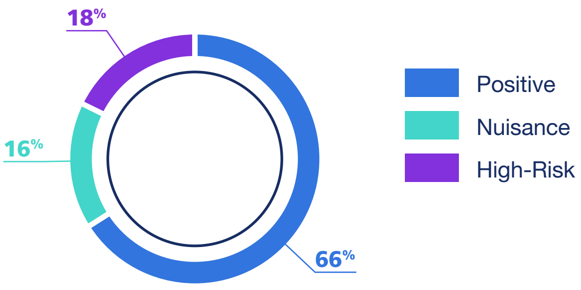
VoIP networks make it relatively easy to spoof caller ID. While most unwanted calls continue to originate from VoIP numbers, the percentage of *legitimate* calls went *up* to 83% in 2020, rising from 66% in 2019.

TNS believes this is partially due to efforts by large operators to identify unwanted traffic from interconnect partners and successfully shutting down bad traffic. It's also likely due to the increased propensity to spoof toll-free numbers.

Scoring of VoIP Telephone Numbers—2020



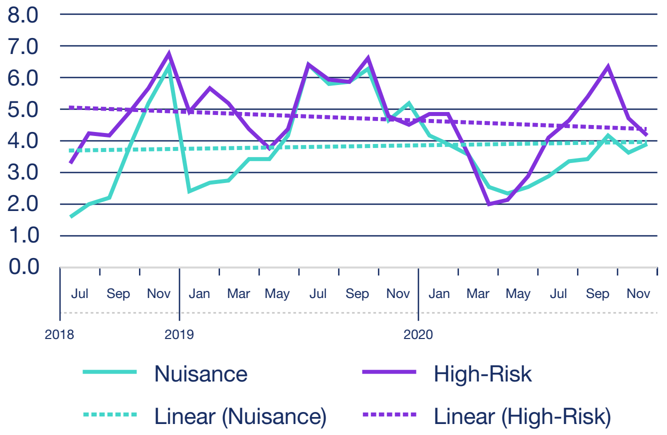
Scoring Distribution of VoIP Telephone Numbers—2019



Unfortunately, bad actors can use VoIP originating networks as well. Still, the number of nuisance calls, on a per subscriber basis, coming from a VoIP telephone number decreased 23% in 2020.

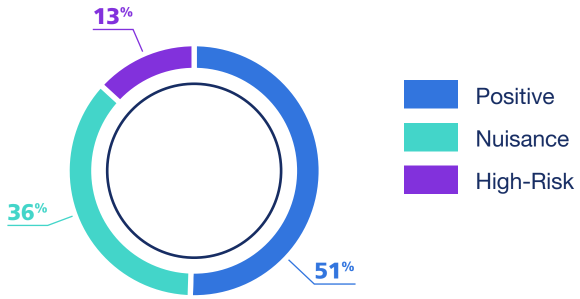
In addition, the number of high-risk calls, on a per subscriber basis from VoIP numbers has decreased 20% in 2020.

Unwanted Calls per Telephone Number—VoIP



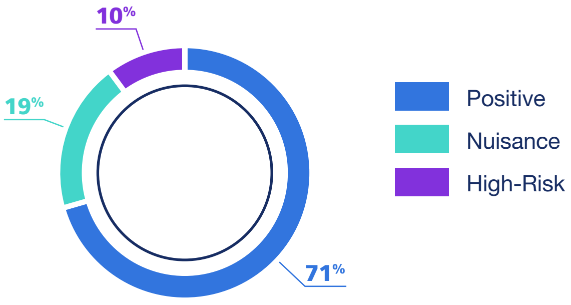
The percentage of positive calls coming from toll-free numbers has increased from 37% in 2019 to 51% in 2020. The decrease in nuisance calls and increase in positive calls is due to an increase in enterprise and government agencies registering toll-free numbers.

Scoring Distributon of Toll-Free Calls—2020



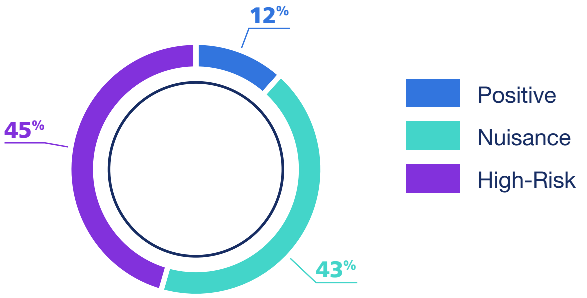
Of the top 10 toll-free numbers in 2020 in terms of volume, 29% of the calls are scored as nuisance or high-risk by TNS, down from 36% in 1H2020.

Scoring of Top 10 Toll-Free Numbers by Volume



The source data from the top 10 toll-free numbers, however, is overwhelmingly considered nuisance or high-risk by the subscriber. The spoofing of legitimate toll-free numbers has made the subscribers suspect of the caller intention.

Crowd-Source Sentiment of Top 10 Toll-Free Numbers



Subscriber sentiment suspect of toll-free numbers

The SHAKEN framework was developed by the ATIS-SIP Forum IP-NNI Task Force, a call authentication framework developed by the industry designed specifically to mitigate unwanted robocalls by reducing the impact of caller ID spoofing. 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.[13]

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

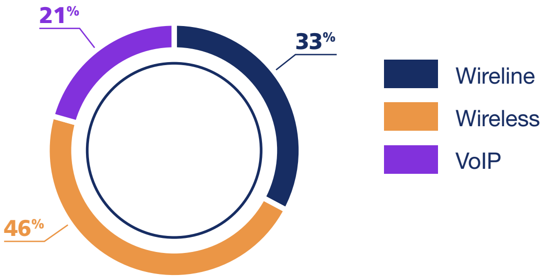
TNS sees this as a potential area a bad actor can exploit in the SHAKEN framework and will continue to work with the industry to remedy this issue.

Termination of Unwanted Calls

Total calls to wireline and VoIP telephone numbers is roughly equal to the number of calls to wireless 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 46% of the total call volume for 2020, unchanged from the previous findings in 1H2020.

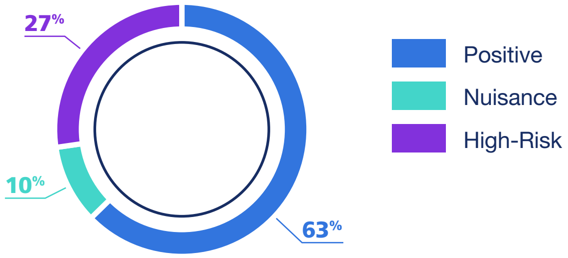
Total Call Distribution—Called Telephone Number



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

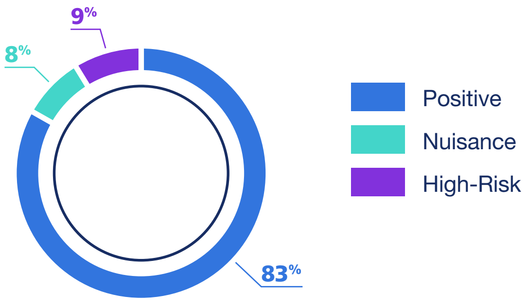
Wireline telephone numbers are twice as likely to receive an unwanted call than a wireless one. The charts show the distribution of call types for 1H2020. Inter-carrier unwanted calls to wireline numbers are 37% of the total call volume; high-risk calls are more than two-and-half times the call volume of nuisance calls.

Distribution of Scoring for Wireline Telephone Numbers



Inter-carrier unwanted calls to wireless numbers are only 17% of the total volume and high-risk calls and nuisance are split evenly at 9%.

Distribution of Scoring for Wireless Telephone Numbers



[13] https://www.atis.org/01_strat_init/dlt/docs/shaken-faq.pdf

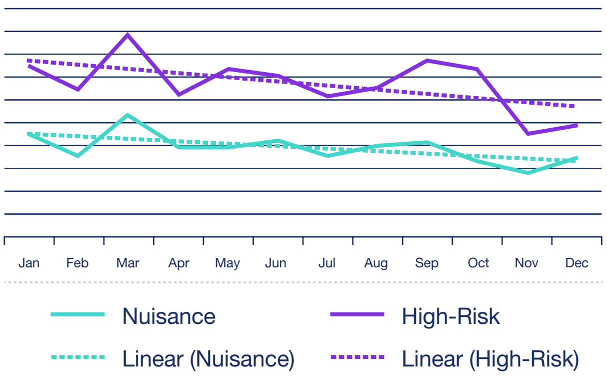
Wireline twice as likely to receive an unwanted call than wireless

The percentage of unwanted calls to wireline numbers dropped from 40% in 1H2020 to 37% for all of 2020. Similarly, the percentage of unwanted calls to wireless numbers dropped from 20% in 1H2020 to 17% for all of 2020.

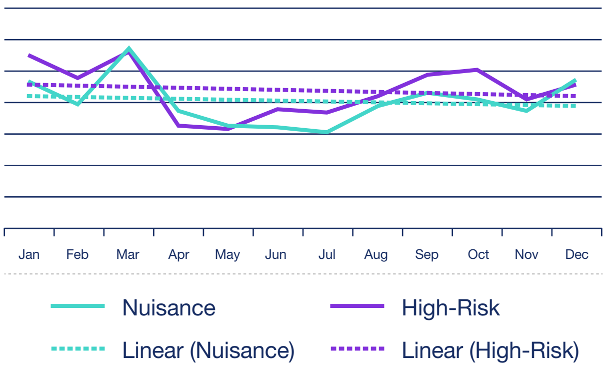
In addition, the total number of unwanted calls to wireline numbers dropped 15% from 1H2020 to 2H2020, while the total number of unwanted calls to wireless numbers dropped by 19% in the same period.

The percentage drop for nuisance calls from this time was similar for wireline numbers (-17%) to wireless numbers (-16%). However, the decline in high-risk calls from 1H2020 to 2H2020 fell more quickly for wireless (-22%) than for wireline (-14%).

Wireline Unwanted Call Trend



Wireless Unwanted Call Trend



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

The major *wireless* providers offer call blocking and labeling services on an *opt-out* basis.[14]

- AT&T Wireless offers *Call Protect* for free
- T-Mobile offers *Caller Screener* for free for Android users and Scam Shield for post-paid users
- Verizon Wireless offers *Call Filter* for free

However, the major *wireline* providers offer call blocking and labeling services on an opt-in basis.[15]

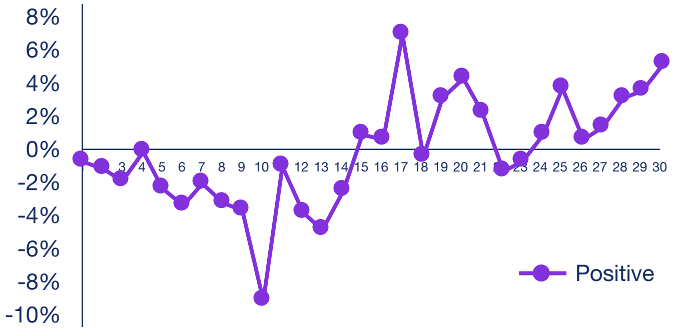
- AT&T offers *Digital Phone Call Protect* for free
- CenturyLink offers VoIP customers a free blocking service
- Charter offers their VoIP residential subscribers a free blocking service
- Comcast offers their VoIP residential subscribers a free blocking service
- Verizon offers two free solutions,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

In addition, the FCC has also been aggressive in enforcing action against illegal robocallers including against gateway providers that facilitated COVID-19-related scam robocalls.[16]

COVID-19 Impact on Scams

As mentioned earlier, bad actors struggled with the shutdowns and a shift to WFH. TNS saw a drop in both unwanted and wanted calls starting in mid-March. Legitimate call originators were able to resume calling their subscribers in mid-April. The following chart shows the week-over-week changes in calling activity.

Call Guardian Change in Positive Calls—April 2020

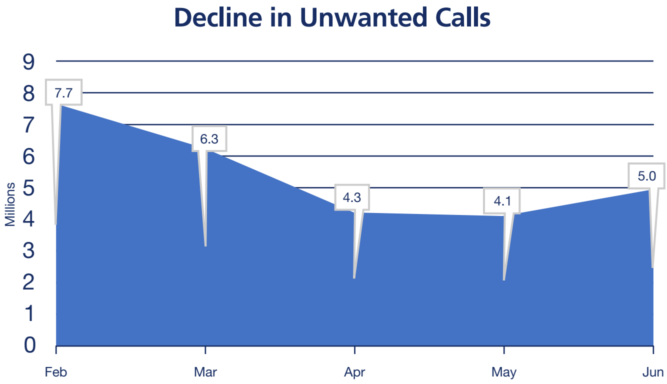


[14] https://www.fcc.gov/document/call-blocking-report-tools-now-substantially-available-consumers

[15] https://www.fcc.gov/document/call-blocking-report-tools-now-substantially-available-consumers

[16] https://www.fcc.gov/document/call-blocking-report-tools-now-substantially-available-consumers

For bad actors, TNS saw a declining trend of unwanted calls continue into April and May before finally reversing in June.



TNS did see the bad actors adjust their scams, shifting to COVID-19 as the topic. COVID-19 scams continued to increase and have the following themes:

Tests or Cures—Selling phony products with claims to prevent, treat, mitigate, detect or cure the virus.

Cleaning—HVAC duct cleaning to "protect" your home and family from the virus.

Retail discounts—Free Netflix for five months, free iPhone 11, free goods from Costco—*"$130 in goodies from Costco! That's our stimulus package for our loyal customers."*

Health insurance—Cheap health insurance that covers coronavirus.

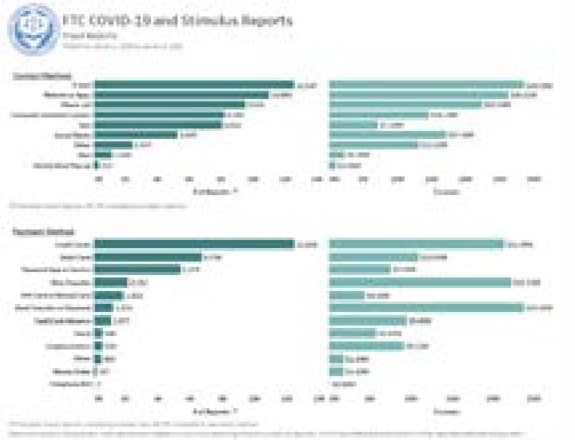
Student loans—New measures included waiving interest on your federal student loans until further notice.

Interest rate reductions—Reducing your interest rate to 0% or eliminating your payments and interest rates due to coronavirus.

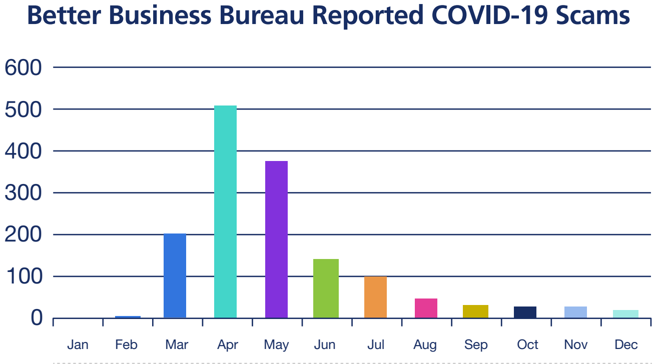
The Netflix, iPhone and Costco scams were texts from 10-digit phone numbers. A recent robotext scam was tied to the IRS stimulus refund check. Please note how the website looks like a legitimate IRS website, but look more closely at the URL

COVID-19 scams extended to robotexts

The FTC reported almost 300,000 incidents due to COVID-19 and stimulus checks during 2020 amounting to over $253 million in fraud loss. Phone calls ranked third in the method of contact, resulting in $22.5 million in losses.[17]



In addition, the Better Business Bureau (BBB) reported a dramatic increase in the number of COVID-19 scams at the beginning of the pandemic and then saw a steady decline as consumers became more aware of these scams. The chart shows the data according to BBB Scam Tracker.[18]



Top Scams

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

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

[17] https://www.ftc.gov/enforcement/data-visualizations/explore-data

[18] https://www.bbb.org/scamtracker/

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 financial information. You should never provide anyone with your personal financial information unless you are sure they're legitimate. Validating this is as simple as asking the caller for a name, company, street address, telephone number and professional license number.

Political scam—These scams took on three forms:

1. **Voter Registration—**In a voter registration phishing attack, scammers may claim you are not registered, but you can register with them over the phone or suggest you are unable to vote because your registration is incomplete.
2. **Cash Donations—**Scammers impersonate or spoof legitimate political campaigns to gain your credit card information.
3. **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.

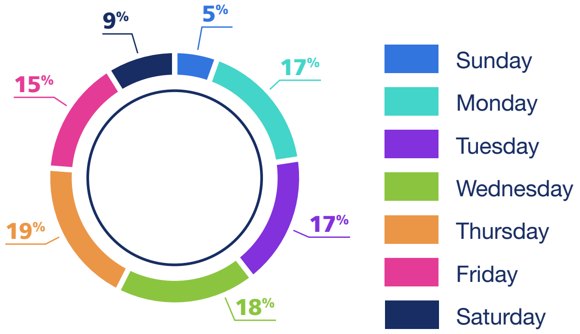
Technology scam—These scams involve the bad actor using the legitimate toll-free number for AppleCare, Amazon or another technology company telephone number to tell you there is something wrong with your account to get your personal information. A technology company will not ask for your password or other personal information.

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.

Healthcare scam—This scam involves using the legitimate toll-free number of the Health Insurance Marketplace offering free or reduced insurance rates to get your personal information.

The number of unwanted calls varies daily with the highest volume of unwanted calls on Thursday during 2020 (19%). The weekend represented 14% of the total volume of calls, a slight increase from 12% in 2019 and 2018.

Day of Week for Unwanted Calls



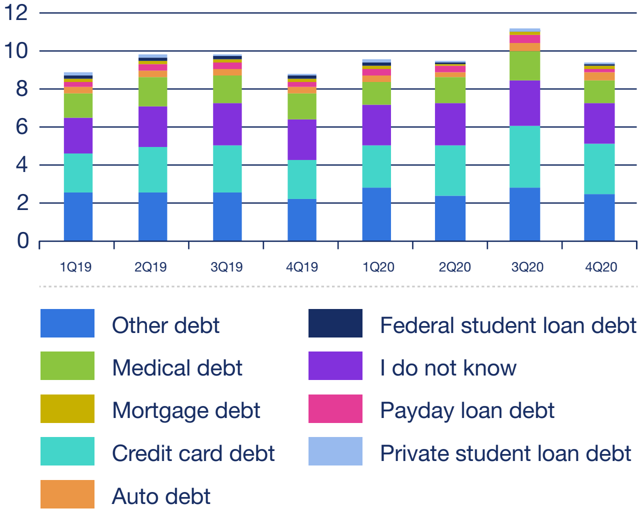
Credit card reduction scam had highest volume on heaviest day in 2020

The day with the highest volume of unwanted calling occurred on March 11, 2020 involving a credit card scam offering an APR reduction.

The **Consumer Financial Protection Bureau** (CFPB) has a database of complaints about consumer financial products and services that that are submitted to the CFPB by consumers and then sent from the CFPB to financial institutions for response. Data from the **Consumer Complaint Database** shows a 6% increase in the number of complaints from the 2019 to 2020. The biggest increase in complaints is from credit card debt, up 19%. Complaints from federal student loan debt and private student loan debt have decreased over 30%.[19]

Approximately 10% of debt collection complaints were about communication tactics. In these complaints, frequent or repeated calls—be it several calls placed in short succession or repeated calls over a longer time period—was the most common issue identified by consumers. Some consumers reported having previously requested that the collector stop calling, which was later ignored. In addition to the frequency of calls, consumers complained about the quality of interactions once they were on the phone with a debt collector. For example, consumers described collectors who were rude or aggressive. In these situations, consumers often escalated the issue and requested that the debt collector connect them with a supervisor.[20]

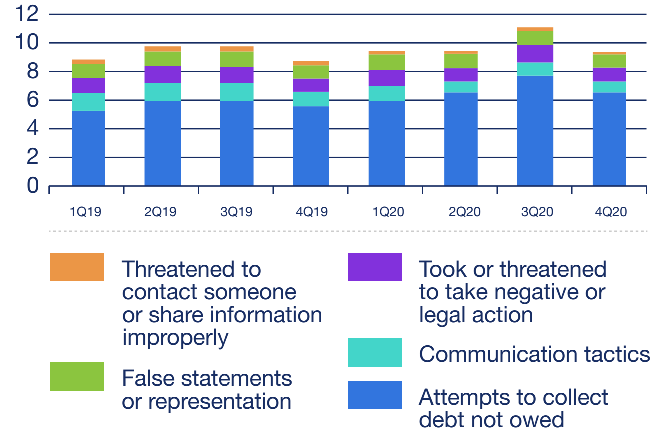
Complaints to Consumer Financial Protection Bureau by Type of Debt



[19] https://www.consumerfinance.gov/data-research/consumer-complaints/
[20] https://www.consumerfinance.gov/data-research/research-reports/2019-consumer-response-annual-report/

The top complaint, by far, *"Attempts to collect debts not owned,"* increased to 18% in 2020, up from 11% in 2019. This may be attributed to the debt collection scams purported by the bad actors rather legitimate first-party debt collectors. *"Threatened to contact someone or share information improperly"* saw the biggest drop in number of complaints year-over-year.[21]

Complaints to Consumer Financial Protection Bureau by Issue

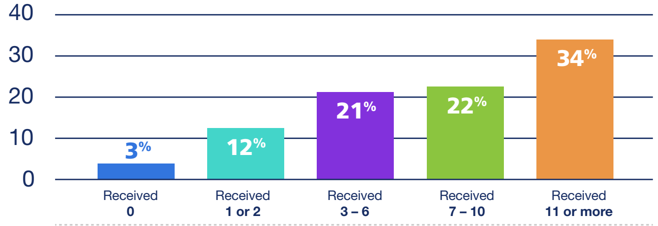


TNS conducted a survey in first half of 2020 and found that 53% of US senior citizens believe robocallers tried to scam them out of personal information in 2019; and nearly as many (47%) reported that they were targets of financial scams in 2018.[22]

Additional findings from the survey are the following:

- **Robocall volume is high among seniors.** Eighty nine percent 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 coronavirus 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 a robocall protection app—suggesting an opportunity for carriers to broaden app branding and education efforts.

Robocalls per Week



Robocall Impacts on Primaries and Presidential Election

With 2020 being a Presidential election year, voters were targeted for political robocalls. Several states had primaries early in the year, led by Iowa, New Hampshire, Nevada and South Carolina. Super Tuesday occurred on March 3 where 16 states held their primaries.

Not surprisingly, these early states saw a significant number of robocalls compared to a typical week. Almost every state saw a rise in robocall activity ranging from nearly 150% to over 600%. Only one state saw a decline, Alabama.

The frequent changing of primary dates due to COVID-19 posed an opportunity for bad actors to confuse voters with calls saying the date was changed when it wasn't or providing incorrect new dates or instructions.

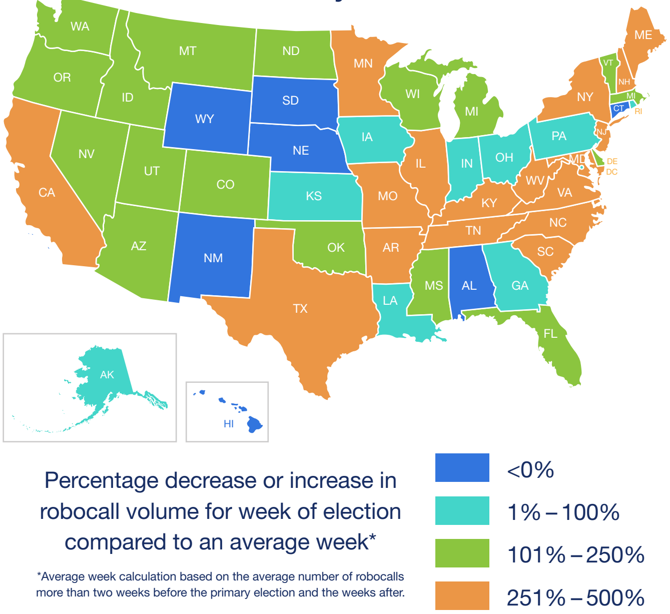
One scam in Texas highlighted a Republican political effort designed to cause confusion over the date of the Democratic primary. More than 75,000 calls were placed and the caller was based in San Antonio.

By the end of March, events covering well over 50% of each party's delegates had taken place and robocall volume slowed down slightly. But the call volume increase ranged between 100%-200%.

As the Democratic candidate became apparent, more states experienced declining fraudulent calls. However, some states still saw an increase in call volume, but was not more than 130%.

The infographic below shows how each state stacked up.

Volume of Robocalls for the Week of Primary Election



Percentage decrease or increase in robocall volume for week of election compared to an average week*

*Average week calculation based on the average number of robocalls more than two weeks before the primary election and the weeks after.

[21] https://www.consumerfinance.gov/data-research/consumer-complaints/

[22] https://tnsi.com/robocallers-tried-to-scam-nearly-half-of-senior-citizens-out-of-money-in-2019/

The race to the Presidential election saw an even more dramatic increase than the primaries. Political calls accounted for approximately 10% of the unwanted call volume from July to October.

The states that saw the largest number of political calls per population, for the last for weeks leading up to the election, were the following:

1. Montana
2. North Carolina
3. Wisconsin
4. Maine
5. Iowa

Montana, North Carolina, Maine and Iowa saw an increase between 200-700% for the general election in November compared to their primaries. Wisconsin saw a mind-boggling 2,300% increase and averaged over 1.2 million calls per week leading up to the November election.

TNS conducted a survey on political calls at the end of 2020 and found that 45% of respondents received more than six calls in the month leading up to the election. Younger adults (25-to-30-year-old) were the most targeted (62%) demographic receiving a robocall/robotext on election day versus the national average of 51%.

Additional findings from the survey are the following:

- **Voters now they are being hit with disinformation.** In 2020, 43% of the respondents thought that they received a robocall/robotext that they believed contained false or misleading information about the election. What's more, 54% believed robocalls/robotexts were used to try and undermine confidence in the 2020 Presidential election.
- **Branded calling would help answer rates.** More than 40% of respondents said they would be more likely to answer a political robocall if their caller ID showed the name of a political party/candidate/organization instead of just an unknown phone number.
- **Most voters aren't engaging with suspicious robocalls/robotexts.** While 51% of Americans thought that it was hard to tell the difference between a legitimate election robocall/robotext and one with misinformation, only 24% engaged with the robocall/robotext.

The end-users of TNS services provide direct feedback through the mobile device and for the days leading up to the election, November 1-4, political calls clearly stood out based on word cloud analysis.

political
scam
spam
number
calling
text
phone
know
stop
scammer
dont
election
phishing
unknown
apple
unsolicited
insurance
harassing
day
icloud

During October, end-users said these subjects were the leading robotext topics based on word cloud analysis.

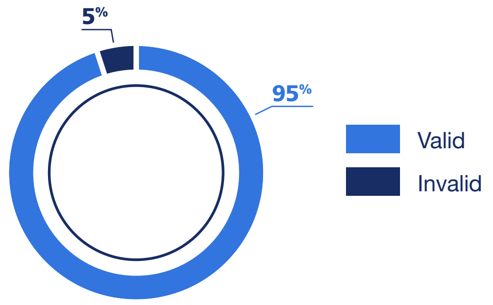
political
spam
stop
messages
unsolicited
#phishing
phone
unwanted
number
#scam
scam
scammer
block
fedex
#text
calls
calling
received
#spam
numbers
different
call

Finally, consumers with Georgia telephone numbers saw 300% increase in political calls for the Georgia Senate run-off as compared to the Presidential election. The call volume just in Atlanta Metro saw a 50X explosion in the number of political calls compared to the rural areas of Georgia on a per population basis.

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 significantly decreased by 35% in 2020. It is important to note that invalid / unallocated numbers remain a small percentage of total unwanted call volume (5%).

Unwanted Calls by Valid/Invalid NPA-NXX



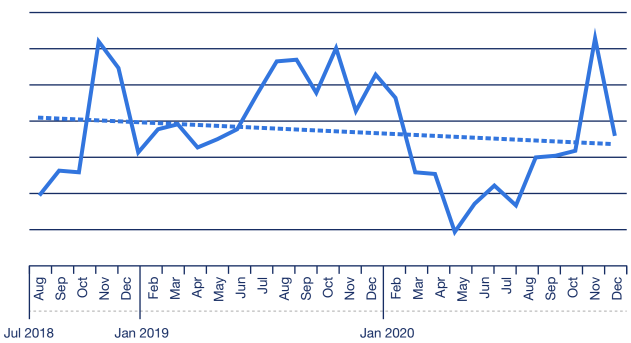
US election cycle fueled a spike in misinformation campaigns

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

TNS expects this trend to continue to slow as voice providers begin to implement network call blocking.

Invalid Calls per Telephone Number



Invalid telephone numbers are a small part of the problem and declining

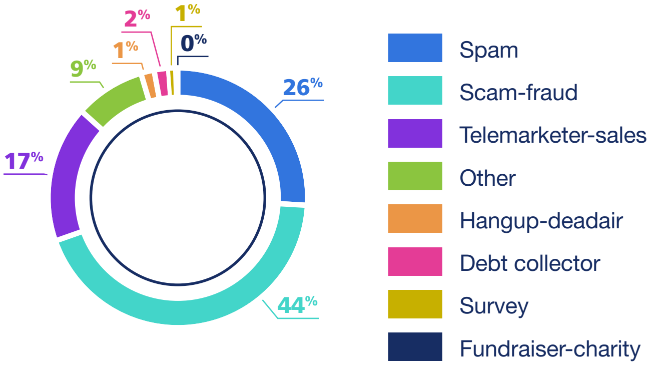
Crowd-Sourced Statistics

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

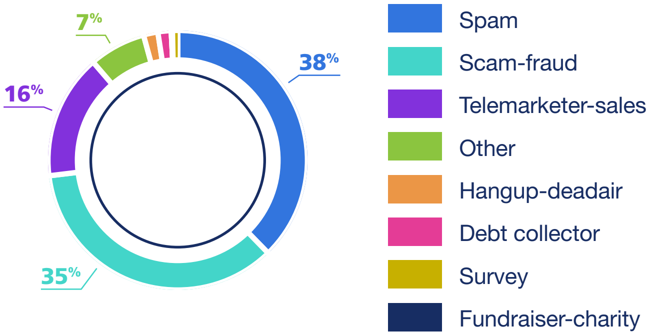
Enhanced Caller ID identifies callers or texters with their names displayed directly in the incoming call screen and message threads, even if their number is not in contacts.

The end-users of TNS services provide direct feedback through the mobile device and they have classified their robocalls in the following categories: About 75% are classified as spam or scam-fraud, and 15% are marked as telemarketing-sales. This has been consistent from 2018 through the first half of 2020. However, for 2020, more feedback has come in as scam-fraud at 44%.

Crowd-Sourced Feedback by Major Category—2020

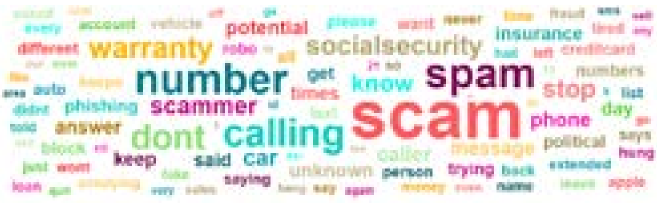


Crowd-Sourced Feedback by Major Category 2018-2020



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

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



End-users will also use hashtags to share information about the call. The top tags used for 2020 were:

1. #scam/#scammer
2. #phishing
3. #spam
4. #telemarketer
5. #robocall

Neighbor Spoofing

TNS launched its **Neighbor Spoofing** feature in mid-2018 and has continued to evolve it to protect consumers from this popular tactic.

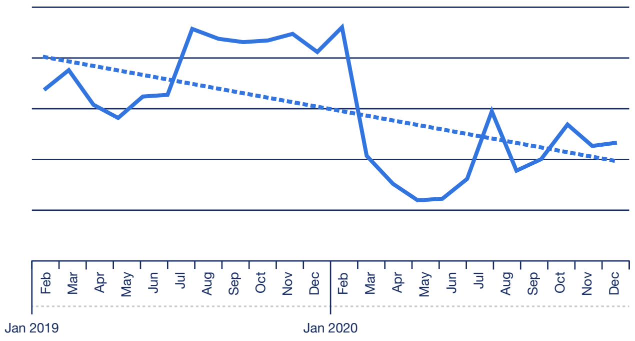
With Neighbor Spoofing, no matter where the call originates, the information on the receiver's phone matches or closely matches the area code and several digits like one's own phone number—which makes the consumer more likely to trust the call and answer.

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.

The combination of deep carrier network integration combined with real-time intelligence of Call Guardian is why TNS is leading in combating this tactic.

TNS has seen a decrease of 43% in neighbor spoofing on a per subscriber basis from 2019 to 2020, however the second half of 2020 saw a slight increase.

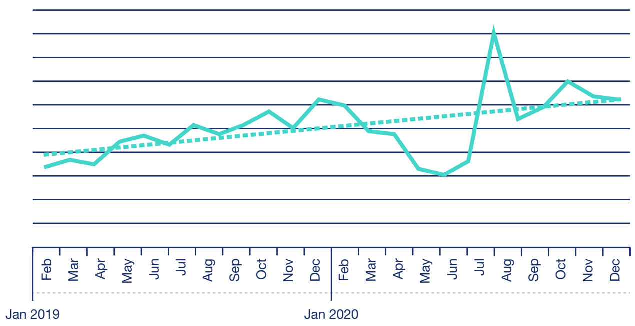
Neighbor Spoofing Events per Subscriber



Bad actors are using neighbor spoofing less due to implementation of STIR/SHAKEN on the major wireless networks. They have shifted to near neighbor spoofing where the area codes are the same, but not the first five or six digits.

Using the same area code has increased 17% from 2019 to 2020. In our previous report, we noted the that the increase was only 7% when comparing 1H2019 to 1H2020.

Near-Neighbor Spoofing Events per Subscriber



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

Near-neighbor spoofing increased with the implementation of STIR/SHAKEN across Tier-1 carriers

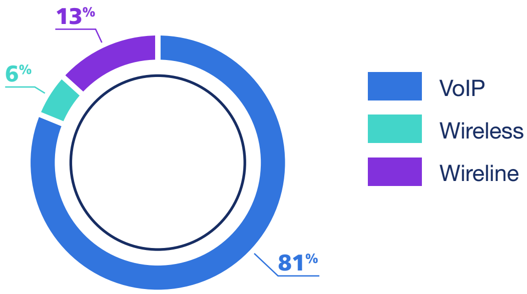
Snowshoe spamming is difficult to detect for over-the-top (OTT) applications. To be effective an application must be integrated with the network and see the cross-carrier events of both the calling number and the called number.

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

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

Near-neighbor spoofing shows that bad actors primarily use VoIP telephone numbers—over 80% of the call volume versus only 6% for wireless telephone numbers. The data in the pie chart below is based on call volume from January 2019 through December 2020.

Near-Neighbor Spoofing by Line Type

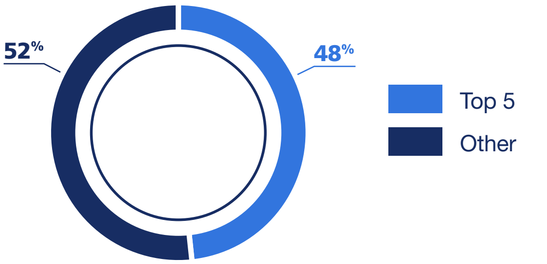


STIR/SHAKEN Attested Traffic

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

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

Cross-Carrier Traffic Among Tier 1 Carriers



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

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

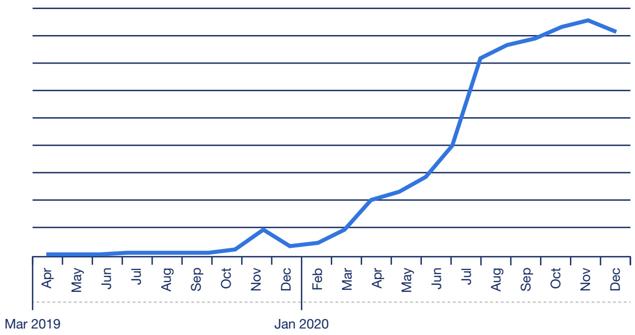
Full Attestation (A)—The service provider has authenticated the calling party and they are authorized to use the calling number.

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

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

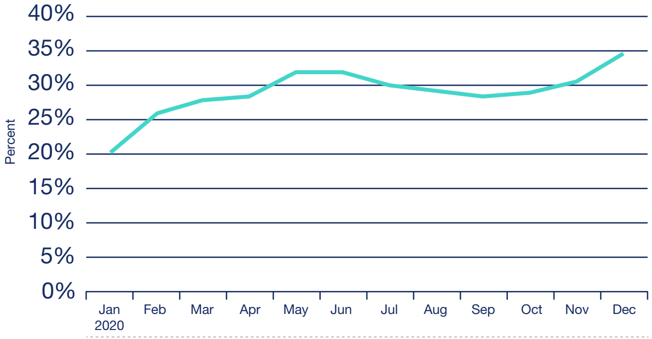
The amount of inter-carrier traffic that TNS has seen that shows attestation has grown dramatically in 2020.

Inter-Carrier Signed STIR/SHAKEN Traffic



TNS estimates that the percentage of calls showing attestation has grown from 21% of the total traffic in January to 35% in December.

STIR/SHAKEN Traffic to Total Traffic



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

Canadian Results

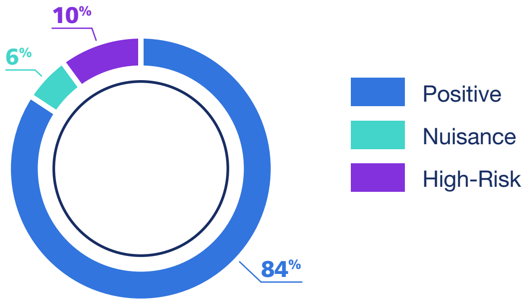
In December 2019, the **Canadian Radio-Television and Telecommunications Commission (CRTC)** mandated universal network-level call blocking. The Commission wanted Canadian carriers and other telecommunications service providers (TSPs) to block numbers when the caller ID numbers don't conform to established numbering plans.

The CRTC expected TSPs to implement this decision within 12 months, or the end of 2020. The mandate, however, does not apply to providers that offer their subscribers call filtering services, which provide more advanced call management features.

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

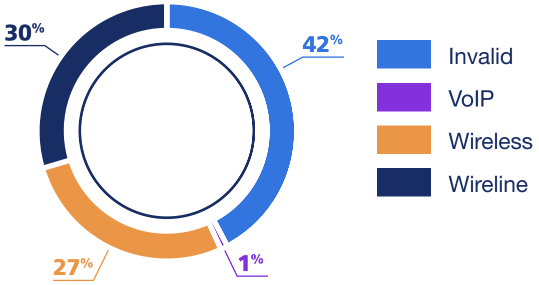
TNS found less than 20% of Canadian inter-carrier calls in 2020 were scored as unwanted, consistent with 2019.

Scoring by Category—Canadian Telephone Numbers



Non-carrier assigned numbers are 42% of the high-risk calls originating from Canadian telephone numbers during 2020. This is a significant decline from 60% in 2019. TNS attributes this to US-based carriers blocking more invalid Canadian area codes.

Distribution of Unwanted Calls from Canadian Telephone Numberss



International Results

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

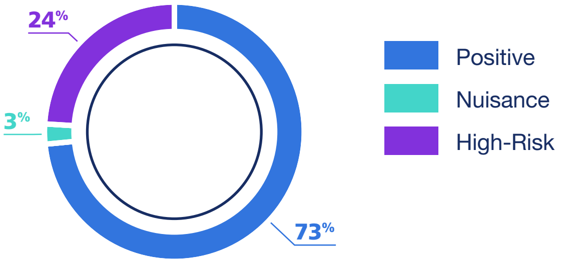
The 2020 data shows 73% of calls from an international number as positive and significantly higher than previous findings. The end of 2020 saw significant number of **Wangiri** attacks coming from the Caribbean.

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

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

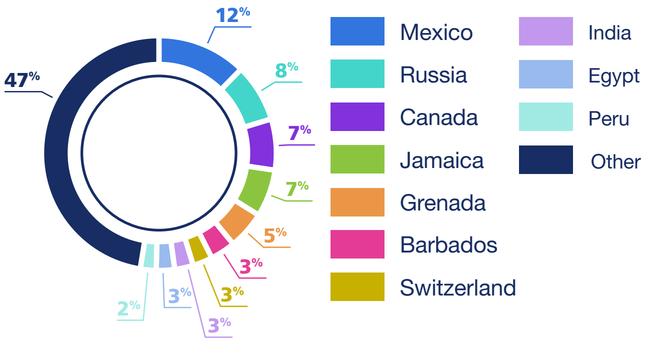
Every time you call, you will be charged high international rates or other connection fees. The bad actor profits from those fees.

Scoring by Category—International Telephone Numbers



The Caribbean Wangiri attacks show up within the top countries that have unwanted calls coming from their numbering resources are summarized below.

Unwanted Calls from Numbers Outside US



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

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

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

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

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

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

Recognize Robocalls are Not Created Equal

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

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

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

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

At the same time, most consumers still want to utilize voicemail for call screening. Almost 70% of consumers want lower-risk calls sent to voicemail, letting them control which messages to return.[23]

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 let go through.

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

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

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

Prioritize Consumer Education

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

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

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

More than 70% of consumers surveyed agree that they would like to use an app from their wireless carrier to identify potential robocalls.[24] 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.

[23] https://tnsi.com/tns-robocall-survey-consumers-want-more-control-or-options-to-combat-robocalls/
[24] https://tnsi.com/tns-robocall-survey-consumers-want-more-control-or-options-to-combat-robocalls/

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

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

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

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

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

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

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

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

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

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

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

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 block unwanted calls by default that is based on call analytics if 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 which allow 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) use 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. It includes the ability to bulk upload telephone numbers and provide any other relevant information that will ensure proper labeling.

Enterprises should work with analytics providers to register their calling campaigns

Don’t Call Unassigned Numbers Frequently

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

Comply with DNC Lists, TCPA and FDCPA

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

Branded Calling

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

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

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

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

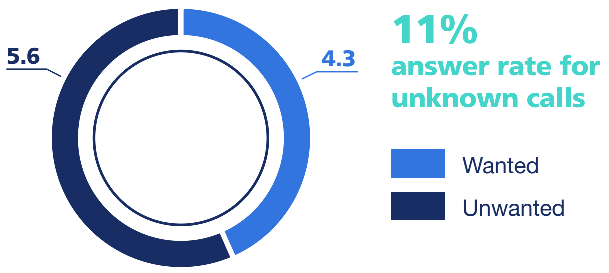
Improving your customer’s trust in your call authentication will help strengthen your brand.

Branded Calling Study

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

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

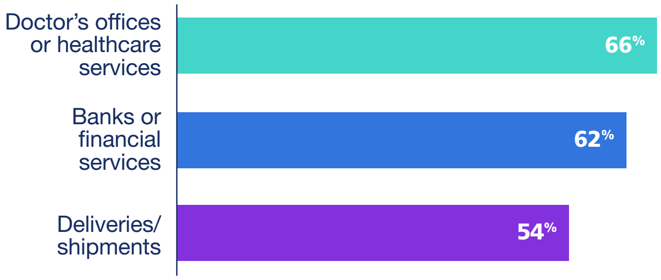
Unknown Calls



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

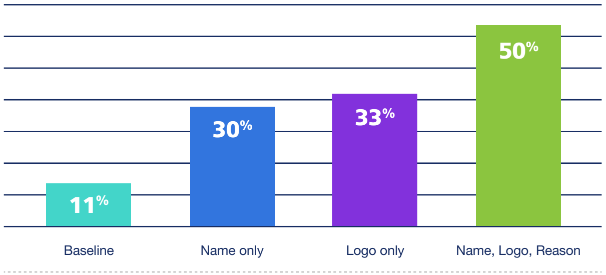
Consumers are most interested in receiving calls from healthcare services, financial institutions and delivery services.

Consumers Most Interested in Calls From



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

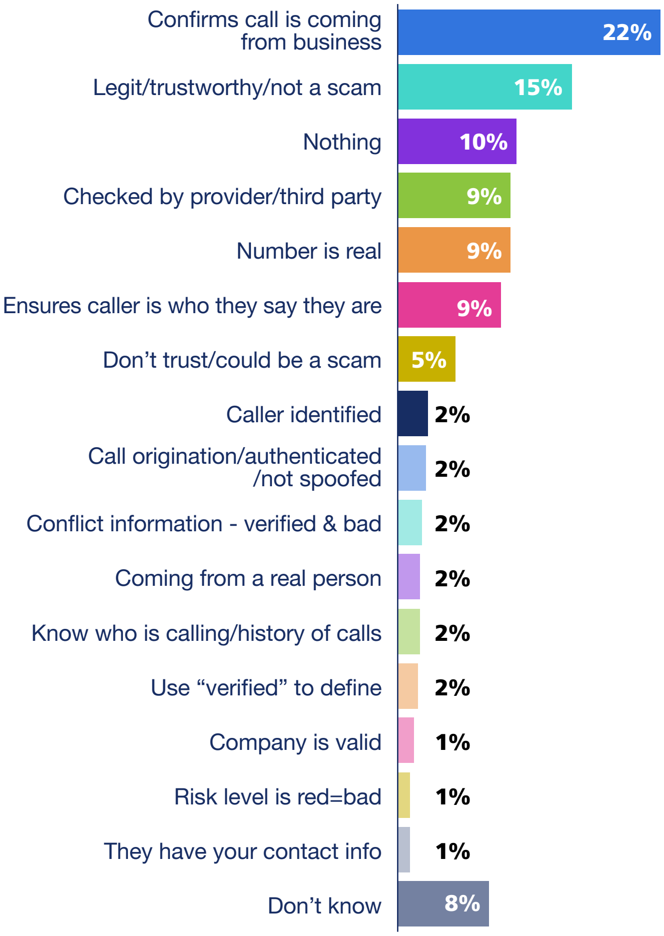
Percent Likely to Answer



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

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

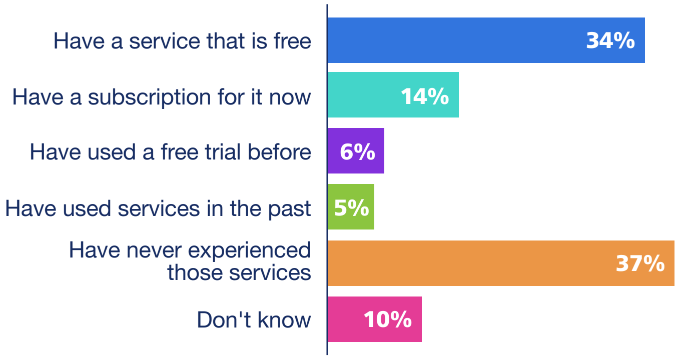
Interpretations of "Caller Verified" Verstat



Call verification is still misunderstood

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

Experience with Caller ID/Caller Protection Services



The FCC was very focused on implementing the TRACED Act in the second half 2020 with a flurry of activity coming in the last week of December.

This section focuses on just the second half of 2020. You can refer to the *2020 1H Robocall Investigation Report* for the actions taken in the first half of 2020.

FCC Issues Third Report and Order, and Fourth Notice of Proposed Rulemaking

In June 2020, the FCC released a draft order and a notice of proposed rulemaking (NPRM). The ***Order*** establishes a safe harbor from liability for terminating voice service providers that block calls based on reasonable analytics designed to identify unwanted calls, so long as those consider information from the STIR/SHAKEN call authentication framework.[25]

The order also establishes a safe harbor enabling voice service providers to block traffic from bad-actor voice service providers that, either negligently or intentionally, continue to allow unwanted calls to traverse their networks.

Finally, the order, requires blocking providers to furnish a single point of contact to resolve unintended or inadvertent blocking and emphasize that they should make all reasonable efforts to ensure that critical calls, such as those from Public Safety Answering Points, are not blocked and that they never block calls to 911.[26]

The *NPRM* seeks comment on call blocking steps and how to further implement the TRACED Act.

The NPRM also proposes to establish an affirmative obligation for voice service providers to respond to certain traceback requests, mitigate bad traffic and take affirmative measures to prevent customers from originating illegal calls.

Finally, the *NPRM* proposes to require terminating voice service providers that block calls to provide a list of blocked calls to their customers on request and at no additional charge.[27]

FCC Designates Robocall Traceback Manager

At the end of July 2020, USTelecom's Industry Traceback Group was selected by the FCC to serve as the official private-led registered Traceback Consortium per Section 13 of the TRACED Act.[28]

Consumer and Governmental Affairs Bureau (CGB) Clarification on Emergency COVID-19 Related Calls

The Consumer and Governmental Affairs Bureau (CGB) clarified that the TCPA's emergency exception also applies to calls or texts made by or on behalf of health care entities that, pursuant to guidance from federal, state or local government officials, communicate with individuals who have tested positive for COVID-19 to encourage them to donate their plasma after recovering.[29]

FCC Releases Draft Order and Notice of Proposed Rulemaking Mandating STIR/SHAKEN and Proposing Additional Measures to Combat Illegal Spoofing

In early September 2020, the FCC announced that it voted on the following order at its September open meeting.[30]

- Require voice service providers to either upgrade their non-IP networks to IP and implement STIR/SHAKEN or work to develop a non-IP caller ID authentication solution
- Establish extensions of the June 30, 2021 caller ID authentication implementation deadline for small voice service providers, voice service providers that are currently incapable of obtaining a "certificate" necessary to implement STIR/SHAKEN, services scheduled for discontinuance, and non-IP networks
- Require voice service providers subject to an extension to implement a robocall mitigation program on the non-STIR/SHAKEN-enabled portions of their networks
- Require all voice service providers to file a certification in a Commission database showing how they are acting to stem the origination of illegal robocalls
- Establish a process by which providers that make early progress on caller ID authentication implementation can obtain an exemption from the June 30, 2021 deadline, as required by the TRACED Act
- Prohibit voice service providers from adding any line item charges to the bills of consumer or small business customer subscribers for caller ID authentication technology, as required by the TRACED Act
- Require intermediate providers to implement the STIR/SHAKEN caller ID authentication framework in the IP portions of their networks by June 30, 2021

[25] https://www.federalregister.gov/documents/2019/06/24/2019-13270/advanced-methods-to-target-and-eliminate-unlawful-robocalls-call-authentication-trust-anchor

[26] https://www.federalregister.gov/documents/2019/06/24/2019-13270/advanced-methods-to-target-and-eliminate-unlawful-robocalls-call-authentication-trust-anchor

[27] https://www.federalregister.gov/documents/2019/06/24/2019-13270/advanced-methods-to-target-and-eliminate-unlawful-robocalls-call-authentication-trust-anchor

[28] https://www.fcc.gov/document/fcc-designates-robocall-traceback-manager

[29] https://www.fcc.gov/document/cgb-clarification-emergency-covid-19-related-calls

[30] https://www.fcc.gov/document/promoting-caller-id-authentication-combat-spoofed-robocalls

FCC Call Blocking Safe Harbor Order Effective October 14

On September 14, 2020, the FCC encouraged call blocking by:[31]

- Establishing a safe harbor from liability under the Communications Act and the Commission's rules for the unintended or inadvertent blocking of wanted calls, so long as such action is based upon reasonable analytics indicating that such calls were unwanted and therefore should be blocked; and
- Enabling voice service providers, under certain conditions, to stop upstream voice service providers that fail to take actions to mitigate illegal calls from using other voice service providers' networks to pass along bad traffic

FCC Adopts New Rules to Combat Spoofed Robocalls

Also, in late September 2020, The FCC adopted new rules requiring voice service providers to:[32]

- Either upgrade their non-IP networks to IP and implement STIR/SHAKEN or work to develop a non-IP caller ID authentication solution
- Require intermediate providers to implement STIR/SHAKEN so that IP calls retain caller ID authentication throughout the call path
- Prohibit carriers from adding a line item to the bills of consumers and small businesses for caller ID authentication technology
- Grants limited extensions of the STIR/SHAKEN implementation deadline to small voice providers, voice service providers that are currently incapable of obtaining a "certificate" necessary to implement STIR/SHAKEN, services scheduled for discontinuance, and non-IP networks
- Stipulate that providers receiving an extension must implement robocall mitigation programs. By requiring robocall mitigation by providers that have not yet implemented caller ID authentication, the rules combat robocalls even from networks that aren't yet capable of participating in STIR/SHAKEN.

FCC Issued a Notice of Proposed Rulemaking (NPRM) to Address Section 8 of the TRACED Act

In early October 2020, the FCC sought comment on how we can best implement Section 8 of the TRACED Act. The Telephone Consumer Protection Act of 1991 (TCPA) restricts certain calls to residential and wireless telephone numbers absent the prior express consent of the called party or an emergency purpose but authorizes the Commission to exempt certain calls from these restrictions. Those exemptions are:

1. Non-commercial calls to a residence
2. Commercial calls to a residence that do not constitute telemarketing
3. Tax-exempt non-profit calls to a residence
4. HIPAA-related calls to a residence
5. Package-delivery related calls to a wireless number
6. Financial institution calls to a wireless number
7. Healthcare related calls to a wireless number
8. Inmate calling service calls to a wireless number
9. Cellular carrier calls to their own subscribers.[33]

FCC Provides Information on Caller ID Authentication Exemption Certifications

On November 9, 2020, the Wireline Competition Bureau (WCB) provided directions and filing information to voice service providers planning to seek an exemption from the Commission's caller ID authentication rules. All certifications and supporting statements will be required to be filed electronically in WC Docket No. 20-68, Exemption from Caller ID Authentication Requirements, in the Commission's Electronic Comment Filing System (ECFS), available at http://www.fcc.gov/ecfs no later than December 1, 2020.[34]

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

FCC Issues One-Ring Scam Order

At the end of November 2020, the FCC permitted voice service providers to block all calls from numbers "highly likely" to be associated with one-ring scams, as identified using reasonable analytics. The FCC also established a safe harbor for inadvertent blocking of lawful calls if identified by reasonable analytics as potential one-ring scam calls.

Opt-out is *not* required for blocking of these calls. Further, the FCC rejected as outside the scope of the proceeding a proposal to permit voice service providers to block a consumer's outbound call to a number associated with a one-ring scam.[35]

[31] https://www.govinfo.gov/content/pkg/FR-2020-09-14/pdf/FR-2020-09-14.pdf

[32] https://www.fcc.gov/document/fcc-adopts-new-rules-combat-spoofed-robocalls

[33] https://docs.fcc.gov/public/attachments/FCC-20-140A1.pdf

[34] https://www.fcc.gov/document/information-caller-id-authentication-exemption-certifications

[35] https://docs.fcc.gov/public/attachments/FCC-20-171A1.pdf

FCC Selects SomosGov as Next Telephone Number Administrator and Reassigned Numbers Database Administrator

In the beginning of December 2020, the FCC selected SomosGov to serve as the North American Numbering Plan Administrator, the Pooling Administrator, and the new role of Reassigned Numbers Database Administrator under a five-year contract, with options for the FCC to continue the contract for up to a total of eight years.[36]

The order extended the statute of limitations during which robocallers can be fined for TCPA and for spoofing violations to four years from one year.

Also, the order increased the maximum fines for intentional robocall violations.

WCB Seeks Comment on Requests for Extension of STIR/SHAKEN Deadline and on Verizon Petition for Declaratory Ruling

On December 4, 2020 the WCB sought comment on four timely-filed extension requests and on a related petition for declaratory ruling filed by Verizon.[37]

FCC Issued a Notice of Proposed Rulemaking (NPRM) to Address Section 10(a) of the TRACED Act

On December 8, 2020, the FCC adopted and released a NPRM that seeks comment on proposed rules to create a process that “streamlines the ways in which a private entity may voluntarily share with the Commission information relating to: ‘a call or text message that violates the law regarding robocalls or spoofing.’” The TRACED Act requires the FCC to establish such regulations no later than June 30, 2021.[38]

Hospital Robocall Protection Group Issues Best Practices

On December 14, 2020, the Hospital Robocall Protection Group met to present a report to the FCC recommending best practices that voice service providers, hospitals, and federal and state governments can follow to prevent unlawful robocalls from disrupting communications in hospitals.[39]

FCC Issues Caller ID Authentication Best Practices

On December 14, 2020, the WCB issued best practices that providers of voice service may adopt as part of their implementation of effective call authentication frameworks to ensure that the calling party on a voice call is accurately identified, as directed by the TRACED Act.[40]

FCC Submits TRACED Act Annual Report 2020 to Congress

On December 23, 2020, the FCC provided a report of information that Section 3 of the TRACED Act requires, including data regarding informal consumer complaints that the Commission received during the preceding five full calendar years (2015-2019), and Commission enforcement actions during the preceding calendar year (2019). The FCC also provided additional informal consumer complaint data and information about Commission enforcement actions through November 30, 2020.[41]

WCB Announces Seven Voice Service Providers Qualified for STIR/SHAKEN Exemption

Also, on December 23, 2020, the WCB announced that seven voice service providers demonstrated that they meet the criteria for an exemption under TRACED Act Section 4(b)(2)(A) and the Commission’s rules:

- AT&T
- Bandwidth
- Charter
- Comcast
- Cox
- Verizon Wireless
- Vonage

Nsight did not qualify for the non-IP exemption.

The following companies filed collectively as Nsight:

- Bayland Telephone
- Borderland Communications
- Brown County C-LEC
- Lakefield Telephone Company
- Net Lec
- Niagara Telephone Company
- Northeast Telephone Company
- Nsighttel Wireless.[42]

[36] https://www.fcc.gov/document/fcc-selects-somosgov-next-telephone-number-administrator

[37] https://docs.fcc.gov/public/attachments/DA-20-1454A1.pdf

[38] https://docs.fcc.gov/public/attachments/FCC-20-174A1.pdf

[39] https://www.fcc.gov/document/hospital-robocall-protection-group-issues-best-practices

[40] https://www.fcc.gov/document/fcc-issues-caller-id-authentication-best-practices

[41] https://www.fcc.gov/document/fcc-submits-traced-act-annual-report-2020-congress

[42] https://www.fcc.gov/document/seven-voice-service-providers-qualified-stirshaken-exemption

FCC Issued Report and Order for Rules and Regulations Implementing the TCPA

On December 30, 2020, FCC adopted measures to implement Section 8 of the TRACED Act. Specifically, the FCC ensured that any exemption adopted pursuant to Sections 227(b)(2)(B) or (C) includes requirements with respect to:

1. The classes of parties that may make such calls
2. The classes of parties that may be called
3. The number of such calls that may be made to a called party.[43]

Amended the TCPA exemptions for calls made to *residential* telephone lines for:

1. Non-commercial calls
2. Commercial calls that do not include an advertisement or constitute telemarketing
3. Tax-exempt nonprofit organization calls
4. HIPAA-related calls

Concluded that the conditions that the FCC has already imposed on exemptions for calls made to *wireless* telephone numbers satisfies the requirements of the TRACED Act and therefore do not require any changes to:

1. Package delivery calls (one notification for each package, with one additional notification for up to two follow-up attempts to obtain a recipient's signature if a signature is needed for delivery)
2. Financial institution calls (no more than three calls per event over a three-day period for each affected account)
3. Healthcare provider calls (one per day, up to three per week)
4. Inmate calling service calls (no more than three notifications following an unsuccessful collect call)

Declined to make any changes to the 1992 ruling that allows cellular carrier calls to their own subscribers.

FCC Issued Fourth Report and Order for Advanced Methods to Target and Eliminate Unlawful Robocalls

Also, on December 30, 2020, FCC issued an order that adopted the following measures:[44]

- Requires all voice service providers to respond to traceback requests from the Commission, civil and criminal law enforcement, and the Consortium
- Requires voice service providers to take steps to effectively mitigate illegal traffic when notified by the Commission
- Requires that all originating voice service providers know their customers and exercise due diligence in ensuring that their services are not used to originate illegal traffic
- Expanded existing call blocking safe harbor to cover network-based blocking of certain if that blocking is based on reasonable analytics that incorporate caller ID authentication information designed to identify calls and call patterns that are highly likely to be illegal
- Adopted rules to provide greater transparency and ensure that both callers and consumers can better identify blocked calls and ensure those that are wanted are un-blocked, consistent with Section 10(b) of the TRACED Act. Requires:
  - Terminating voice service providers that block calls to immediately notify the caller that the call has been blocked by sending either a SIP or ISUP response code. Providers must comply with this requirement by January 1, 2022
  - All voice service providers in the call path to transmit these codes to the origination point
  - Terminating voice service providers that block calls on an opt-in or opt-out basis to disclose to their subscribers a list of blocked calls upon request
  - Terminating voice service providers to provide a status update to the party that filed the dispute within 24 hours when a calling party disputes whether blocking its calls is appropriate
- Broadened point-of-contact requirement to cover caller ID authentication concerns under Section 4(c)(1)(C) of the TRACED Act. Establishes a mechanism for callers that are adversely affected by information provided by the caller ID authentication framework to verify the authenticity of the calls.

The FCC declined to extend redress mechanisms to erroneous call labeling.

[43] https://docs.fcc.gov/public/attachments/FCC-20-186A1.pdf

[44] https://docs.fcc.gov/public/attachments/FCC-20-187A1.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.[45]

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.[46] [47]

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.[48]

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

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

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

STIR/SHAKEN

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

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

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

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

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

In simple terms, each TSP obtains their digital certificate from a 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.

[45] https://www.consumerreports.org/cro/magazine/2015/07/robocall-blocker-review/index.htm

[46] https://blog.truecaller.com/2013/07/18/truecaller-statement/24

[47] http://www.ehackingnews.com/2013/07/truecaller-database-hacked-by-syrian.html

[48] https://apps.fcc.gov/edocs_public/attachmatch/DA-16-1121A1.pdf

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 T**elephone Number Reputation Monitoring** from TNS, allow them to understand how their numbers are being characterized, and when activity triggers unwanted reputational scores.

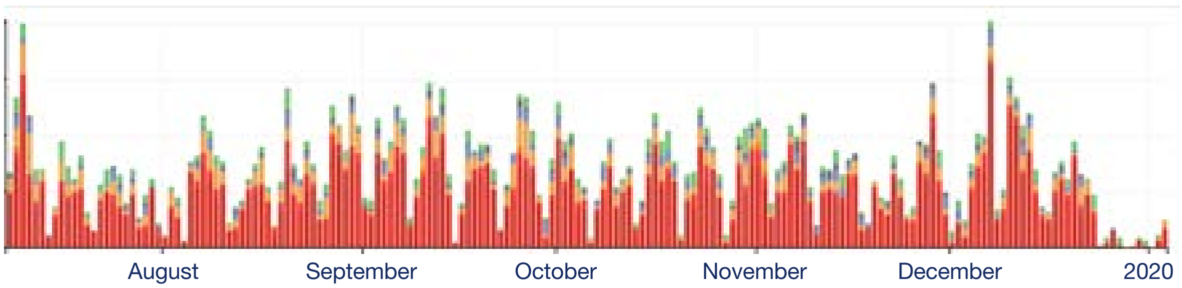
The registration of calling campaigns, for example, will yield positive results, as analytics engines better understand sudden spikes in calling traffic. TNS has seen a dramatic increase in the number of telephone numbers that enterprises have registered through the Reportarobocall website.

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 spikes in calling traffic.

LOGO

Branded calling can restore trust to the voice calling experience



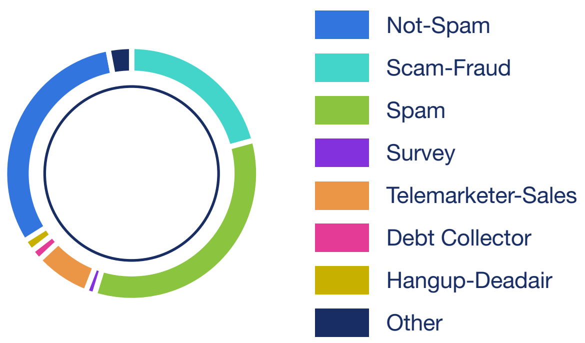
Above is an example showing the mixed customer feedback.

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.

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

Category Distribution



Conclusions and Recommendations

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

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

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.

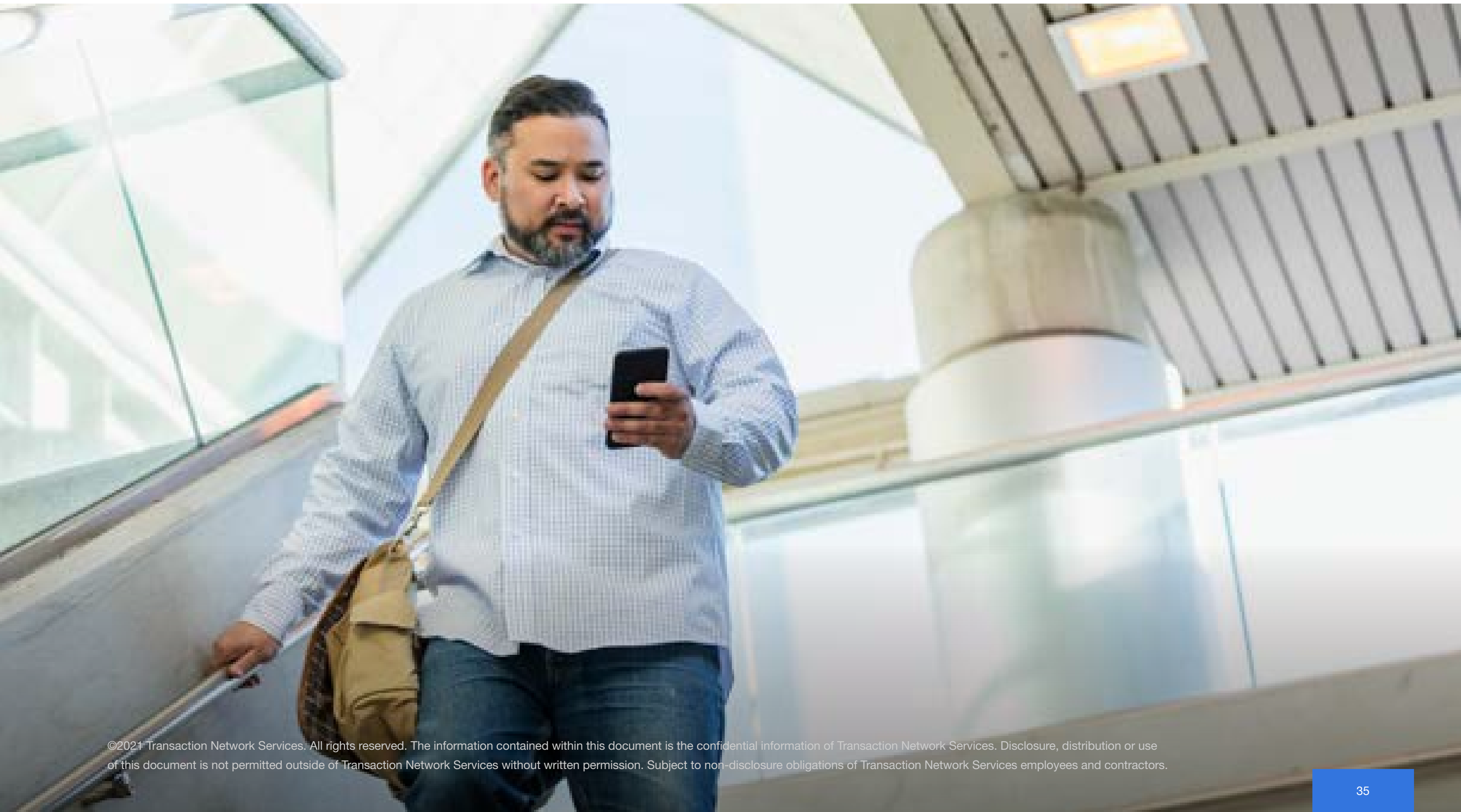
The industry will be looking to the FCC for guidance and support as it seeks to differentiate good calls from bad. More importantly, TNS will seek ways to support the FCC directives by onboarding data from vetted outbound callers and facilitating traceback efforts. It is encouraging to see this problem 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 will publish this report on a bi-annual basis to help the industry improve its security and detection today and adapt to future situations.

A layered approach is most effective in combating robocalls



Transaction Network Services

TNS can help your organization combat Robocalls. Contact us today via phone, eMail or the web.

+ 1 703 453 8300 | solutions@tnsi.com | tnsi.com