Transaction Network Services

One Connection – A World of Opportunities

2018 Robocall Investigation Report

Author: Transaction Network Services

Date: October 2018

Table of Contents

Executive Summary

Robocalling, spamming, scamming, spoofing. This scenario is one that plays out for consumers multiple times a week - if not every day, given that robocalls remain the number one complaint by volume to the FTC and FCC. In fact, an FTC report indicates that the Agency received 4.5 million robocall complaints in 2017, up from 3.4 million the prior year[1].

Nearly one-third of calls are either high risk or nuisance

The 2018 Robocall Investigation Report draws from over 1 billion daily call events across hundreds of carriers and bases robocall scoring and categorization provided to our partners on this data. TNS Call Guardian, our industry-leading big-data analytics engine, has gained insights and reputation on over 1.3 billion phone numbers and our mobile caller ID solutions have been shipped to over 200M mobile devices across more than 500 makes and models.

Tens of thousands of data points weave together the robocall stories and statistics from across the country. What valuable insights can your organization learn from them? Here is a sample of findings discussed in this report:

VoIP numbers are used heavily by robocallers

- **Nearly one-third of calls are either high risk or nuisance.** Negative calls are evenly split between nuisance calls and high-risk calls, and the rate of negative calling to landline subscribers is more than double wireless subscribers.
- **Negative call activity continued to increase over the last eight months.** Negative call activity has risen almost 15% through the first 8 months of the year.
- **Robocall user feedback has nearly doubled.** Growing consumer frustration with robocalls has translated into users more proactively providing feedback, predominantly reporting spam, scam, or telemarketing calls.
- **Neighbor spoofing has emerged as a preferred tactic.** Robocall scammers believe users are more likely to answer the phone if the caller ID shows a familiar number.
- **Real-time analytics is the key to identifying spoofed call activity.** Advanced machine learning methods for labelling negatively scored robocalls using real-time artificial intelligence in combination with big data gleaned from the network effectively addresses the constantly changing identities of robocallers.
- **VoIP numbers used heavily by robocallers.** 50% of the high risk/nuisance calls originate from VoIP numbers.
- **Robocallers doubling down on invalid numbers.** The use of invalid numbers (such as those with area codes that don't exist) continues to rise, doubling over the first six months of the year.

[1] https://www.ftc.gov/news-events/press-releases/2017/12/ftc-releases-fy-2017-national-do-not-call-registry-data-book-dnc

Introduction

The 2018 Robocall Investigation Report by TNS integrates a vast amount of factual evidence from 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 within the network of our carriers.

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, we have attempted to interpret the robocall trends and hope that your organization and consumers will learn from these findings.

Primer on Telephone Numbers

The North American Numbering Plan (NANP) is a telephone numbering plan that encompasses 25 distinct regions in twenty countries primarily in North America, including the Caribbean and the U.S. territories.

Telephone numbers are not all the same, though they all contain 10 digits (NPA-NXX-XXXX) that represent specific information about a number. The first three digits (NPA) are commonly referred to as the area code. The second three digits (NXX) are commonly called the exchange which represents the central office code. The final four digits (XXXX) are the four-digit station numbers.

There are three entities associated to telephone numbers:

- **Allocators of telephone numbers** – there are two primary sources for managing the allocation of telephone numbers, LERG and 8XX Service Management System (SMS/toll-free).
- **Distributors of telephone numbers** – these are the agencies responsible to sell and provision a telephone number to make and receive calls – telecommunications service providers such as VoIP, Wireline and Wireless providers.
- **Assigned users of telephone numbers** – the people, businesses or spammers who make calls from any given telephone number.

Telephone numbers are not all the same because where a number is allocated from or distributed from might have impact on that telephone number's reputation and some might have a greater likelihood to be a negatively scored robocall.

We will use the following categories of telephone numbers:

- Allocated numbers (genuine numbers)
- Unallocated numbers (unassigned numbers)
- Malformed numbers
- Invalid numbers
- VoIP numbers
- Local numbers (familiar numbers)
- Spoofed numbers
- Legitimate numbers
- Illegitimate numbers

Primer on Robocalling

The Telephone Consumer Protection Act or TCPA was passed by Congress in 1991 to regulate the use of automatic telephone dialing systems ("auto-dialers") and prerecorded 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 towards a consumer's cell phone.

A robocall is a phone call that uses a computerized auto -dialer to deliver a pre-recorded message, as if from a robot. Robocalls are often associated with political and telemarketing phone 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[2].

An estimated one in 10 Americans lost money in phone scams between April 2016 and April 2017

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

Robocalls are popular with many verticals, 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 may also be trying to defraud them.

An estimated one in 10 Americans lost money in phone scams between April 2016 and April 2017, says a recent Harris Poll, parting with an average $430 per person for a national total of $9.5 billion. That marks a 56 percent monetary increase over the previous year[3].

Fraud has become easier for criminals as technology, such as VoIP calling, has enabled both spoofing of a number and robo-dialing, and Americans are more likely to answer unknown calls on their mobile phones.

Many robocalls are not wanted and several methods have been developed to prevent unwanted robocalls. The United States has developed the Do Not Call Registry which was created 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, 2017, the registry had nearly 230 million active registrations,[4] up from about 226 million[5] at the same time in 2016.

However, the lists have been ineffective. 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.[6]

[2] https://en.wikipedia.org/wiki/Robocall
[3] https://theharrispoll.com/cash-clever-smart-tax-time-phone-scams/
[4] https://www.ftc.gov/sites/default/files/filefield_paths/dnc_data_book_fy2017.pdf
[5] https://www.ftc.gov/system/files/documents/reports/national-do-not-call-registry-data-book-fiscal-year-2016/dnc_data_book_fy_2016_post.pdf
[6] https://ieeexplore.ieee.org/document/7546510/

Methodology

By creating an industry-leading big data analytics engine, TNS Call Guardian, we have maintained a strong focus on aiding our calling provider partners as they seek to restore trust in voice calls. Our Call Guardian product analyzes over one billion call events across hundreds of carriers every day and bases robocall scoring and categorization provided to our partners on this data.

TNS ensures that Call Guardian evolves in response to emerging bad actor trends, such as neighbor spoofing and perceives the evolution of bad actor calling tactics as a response to the success the industry is seeing in addressing current bad actor methodologies. Neighbor spoofing is when the information on the receiver's phone matches or closely matches the area code and a number of digits similar to one's own phone number.

TNS can provide this unique intelligence because of the combination of deep network integration into our partner carrier networks combined with a layered approach, along with real-time analytics allows us to provide unique visibility beyond honey traps and blacklists. Our layered approach allows TNS to create accurate and comprehensive reputation profiles differentiating legitimate users of telecommunications services from abusive, fraudulent, and unlawful users.

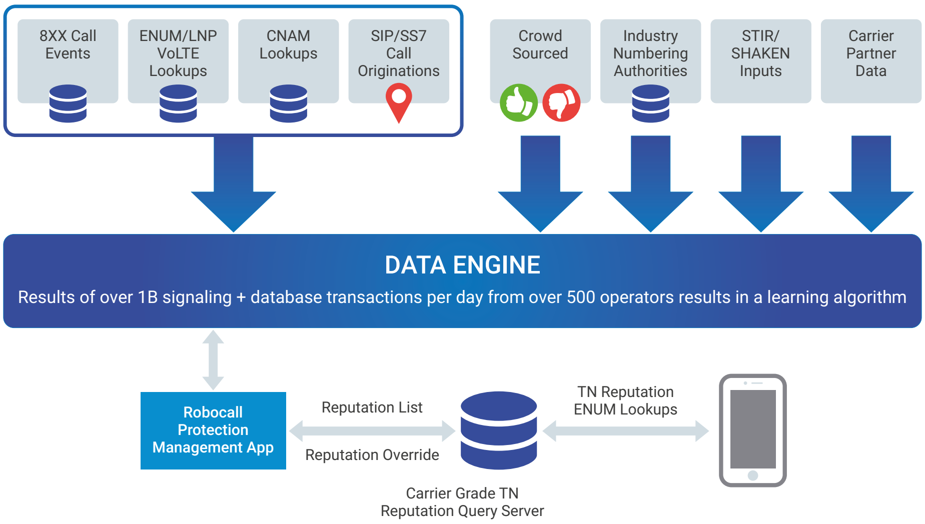
A honey trap or honeypot is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. Generally, a honeypot consists of data (for example, in a network site) that appears to be a legitimate part of the site, but is isolated and monitored, and that seems to contain information or a resource of value to attackers, who are then blocked.[7]

The underlying TNS Call Guardian service architecture is akin to dynamic reputation systems, not to be confused with static list-based reputation systems that contain information of known or previously encountered threats and are typically distributed in the form of blacklists or whitelists. Rather, the service functions similar to a trusted credit reporting service continuously collecting reputation data from multiple sources, relying on a mix of historical reputation 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") for which there is little or no available crowd-sourced reputation data.

Call management and caller identification applications, designed to protect legitimate users of telecommunications services ("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 rely on the service to provide insight that helps identify callers who violate state and federal laws governing the use of automatic telephone dialing systems ("auto-dialers") and caller ID spoofing technologies, most notably scammers who unlawfully use telecommunications services in the commission of a crime of identity theft or fraud and spammers who in willful non-compliance of TCPA, place automated calls, both telemarketing and informational, without the caller's prior consent.

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 to ensure the most accurate reputation score is made available in real-time.

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


8XX Call Events
ENUM/LNP VoLTE Lookups
CNAM Lookups
SIP/SS7 Call Originations
Crowd Sourced
Industry Numbering Authorities
STIR/ SHAKEN Inputs
Carrier Partner Data
DATA ENGINE
Results of over 1B signaling + database transactions per day from over 500 operators results in a learning algorithm
Robocall Protection Management App
Reputation List
Reputation Override
Carrier Grade TN Reputation Query Server
TN Reputation ENUM Lookups

[7] https://en.wikipedia.org/wiki/Honeypot_(computing)

Results and Analysis

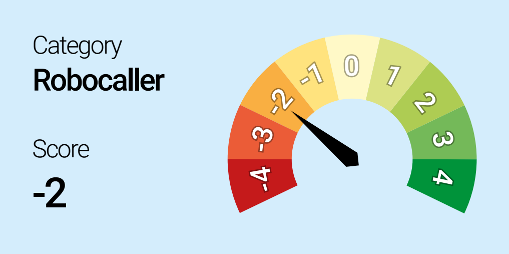
Reputation Category and Scoring

TNS uses reputation categories as a label assigned to telephone numbers observed to have common call behavior. Reputation score provides insight as to the certainty of this categorization and severity of consequences, if any, should an associated threat eventuate.

The below supported reputation categories, generally accepted by the industry, classify the call behavior of hundreds of millions of active telephone numbers. Categories are indicative of legitimate, abusive, fraudulent and unlawful call behavior - inclusive of any call placed with an 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 dispute reputational categories assigned to its telephone numbers.

NORMAL COMPLIANT

Any person or entity with an observed calling behavior falling within the normal behavioral baseline of manually dialed calls - with no abusive, fraudulent or unlawful calling behavior reported. TNs categorized as normal compliant have a reputation score of +1 or greater.



ROBOCALLER

Robocalls are calls made with an autodialer or that contain a message made with a prerecorded or artificial voice. Offenders are normally straightforwardly identified as reputable entities and most commonly place calls with meaningful disclosure of identity.

A positive reputation score (+1 or greater) is assessed to robocallers deemed to have no (or negligible) report of regulatory violations. Examples include utility companies and financial institutions placing robocalls (bill-pay reminders, fraud alerts, debt-collection calls and promotional offers) to customers who have provided prior explicit consent to being contacted by means of their cell phone.

A negative reputation score (-1 or less) is assessed to robocallers deemed to be placing automated telephone calls in a manner that falls below the standard of behavior established by state and federal laws governing the use of auto-dialers. Examples include utility companies and financial institutions that despite having regulatory compliance procedures in place are careless in keeping customer contact information up to date and whose customers disconnect cell phone numbers without notification - resulting in complaints from unintended consumers assigned the affected recycled cell phone numbers.

SPAMMER

Any person or entity placing automated telephone calls, telemarketing and informational, in a manner that might not comply with state and federal laws governing the use of auto-dialers. Regulatory violations are normally difficult to prosecute as there is no meaningful disclosure of identity when placing calls.

A negative reputation score (-1 or less) is always assessed to spammers.

SPOOFER

Any person knowingly and willfully causing transmission of misleading or inaccurate Caller ID info for which there is suspicious behavior but no confirmed report or calling behavior indicative of malicious intent, which otherwise would cause categorization to graduate to potential fraud.

A reputation score of -2 (bad reputation) is assessed to any spoofer having an observed calling behavior that falls within the normal behavioral baseline of manually dialed calls or that are effectively placing calls with an 'invalid' telephone number.

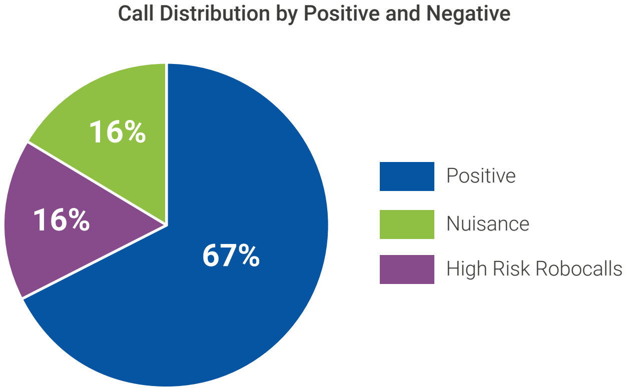
A reputation score of -3 or less is assessed to any spoofer having an observed calling behavior indicative of calls placed with an auto-dialer.

POTENTIAL FRAUD

Any person that appears 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. Typically, deceptive caller ID practices are employed to avoid detection or deceitfully gain caller's trust.

Scoring of Calls

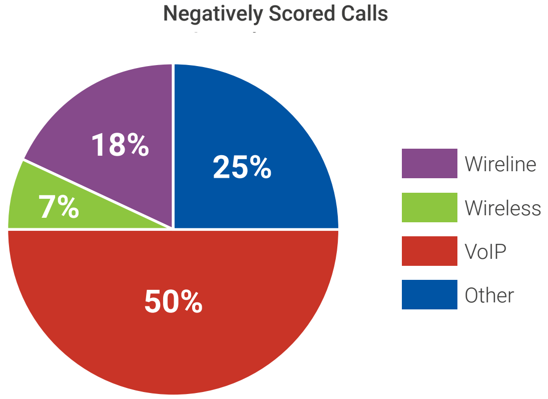
For the first half of 2018, TNS had insight into over 1 billion calls per day and found that roughly a third of the calls were scored negatively as summarized below:



The negative calls are split evenly among nuisance (-2) and high risk (-3, -4).

Origination of Negatively Scored Calls

Not surprisingly, VoIP originated calls generated 50% of the negatively scored calls by total volume.



VoIP originated calls generated 50% of the negatively scored calls by total volume

A provider which allows users to bring their own device and unbundles service so that direct inward dial numbers may be purchased separately from outbound calling minutes will be more flexible. A carrier which doesn't follow established hardware standards (such as Skype) or locks subscribers out of configuration settings on hardware which the subscriber owns outright (such as Vonage) is more restrictive. Providers which market "wholesale VoIP" are typically intended to allow any displayed number to be sent, as resellers will want their end user's numbers to appear.[8]

There are legitimate reasons to modify the calling number, however, bad actors use this same technique to hide their true identity.

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

[8] https://en.wikipedia.org/wiki/Caller_ID_spoofing

Approximately, 2% of the negative calls are from invalid / unallocated numbers and much of the time such calls can be corroborated as spam calls from our crowd-source information.

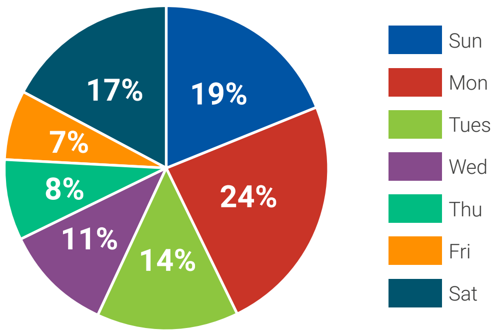
In November of 2017, the FCC adopted rules allowing providers to block calls from phone numbers on a Do-Not-Originate (DNO) list and those that purport to be from invalid, unallocated, or unused numbers.

Monday is the highest day for bad actors

The number of negatively scored calls varies daily with the worst calls (-4) peaking at 10% of the daily volume Monday is the worst for the very bad traffic (-4), while Friday is the lightest day for bad actors.

Most businesses do not typically call their customers on the weekend; however, the bad actors do, which is why the percentage of negative calls to overall calls on the weekend appears high.

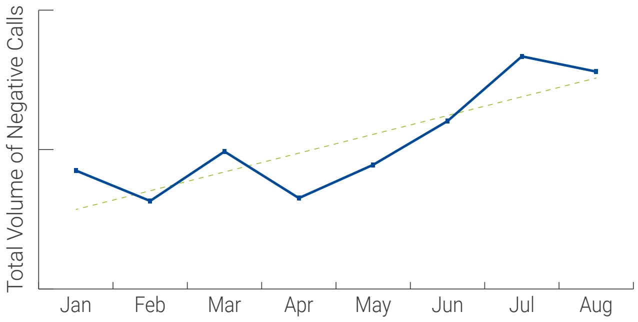
Day of Week for all Negative Calls



Negative Calling Activity

Negative Robocall activity has risen 15% for the first eight months in 2018. TNS expects this trend to continue.

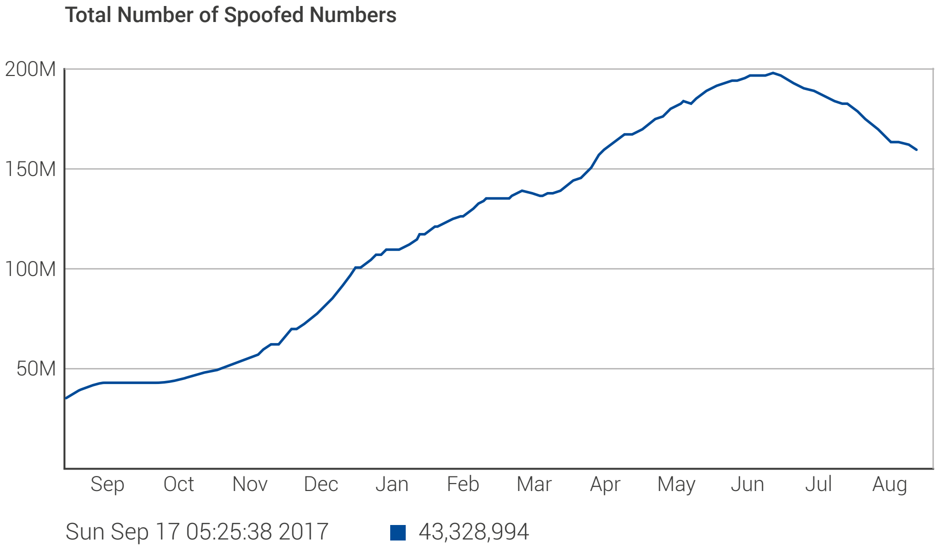
Negative Call Activity Continues to Grow



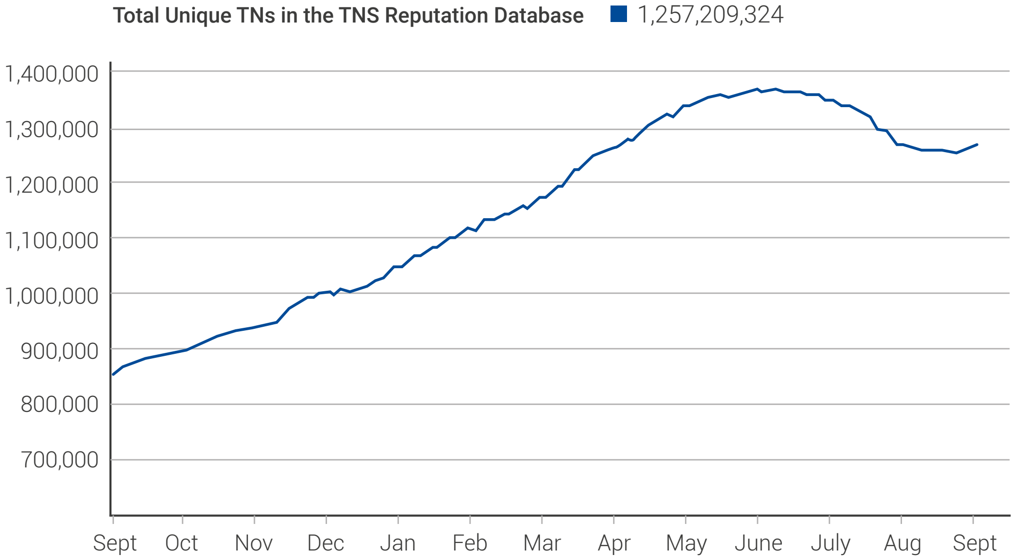
Negative call activity has risen 15%

Invalid/Unallocated Number Use

If those whose work has been focused on detecting and addressing nuisance and illegal robocalls know one thing, it is that bad actors change tactics quickly. Use of spoofed numbers is one of those tactics. Spoofing of invalid/unallocated numbers has increased but is still a small percentage of total negative traffic.



The number of unique telephone numbers in the TNS reputation database is larger than the total number of assigned numbers in North America due to 1.) the use of spoofed numbers and 2.) the broader view of inter-carrier call events TNS processes across its signaling and routing infrastructure where these spoofed numbers can be detected. The number of invalid/unallocated spoofed telephone numbers appears to be falling off, but certain telephone numbers fall off the list only due to inactivity.



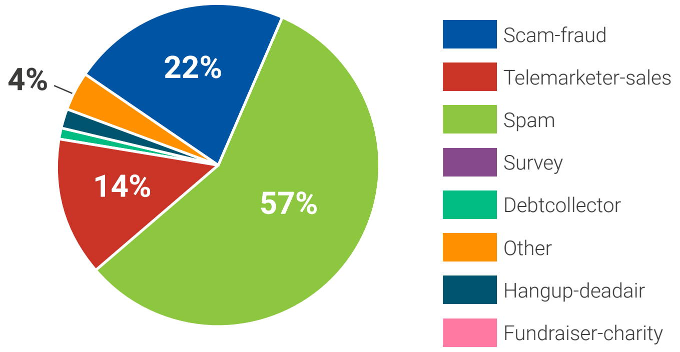
Crowd-Source Statistics

As part of TNS' Identity and Protection portfolio of services, we provide Enhanced Caller ID that is used by the majority of leading US wireless service providers as well as Call Guardian robocall mitigation services to US landline 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 your contacts.

> *Consumers are showing that they want to actively participate and help identify bad actors*

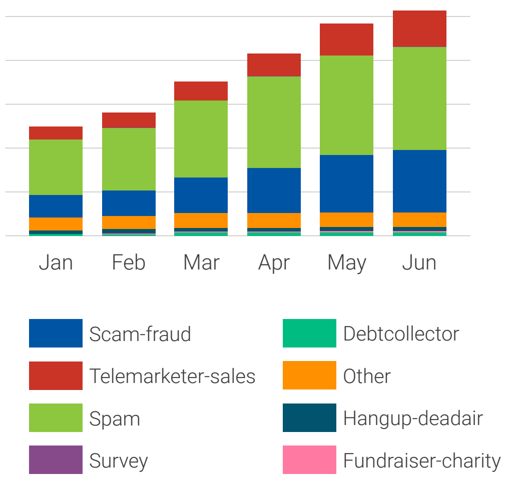
The end-users of this service provide direct feedback to us and they have classified their robocalls in the following categories. More than three quarters of the crowd source data we receive feedback for is classified as spam or scam-fraud.

Crowd Source Statistics by Category



In addition, the amount of crowd source information TNS has received has more than doubled in the first six months of the year. Consumers are showing that they want to actively participate and help identify bad actors.

Crowd Source by Volume



Neighbor Spoofing

TNS launched its Neighbor Spoofing feature earlier this year that enables carriers to protect their subscribers from the increasingly popular neighbor spoofing robocall tactic.

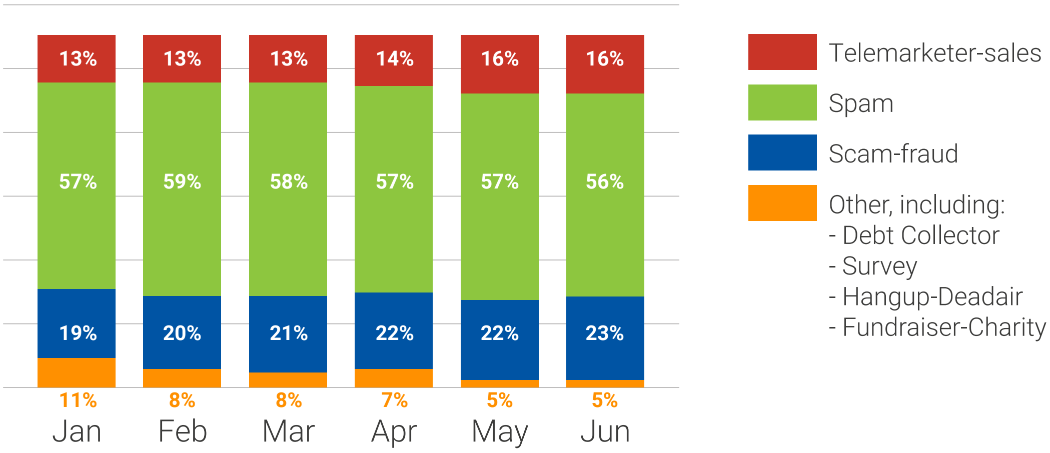
With neighbor spoofing, no matter where the call originates, the information on the receiver's phone matches or closely matches the area code and a number of digits similar to one's own phone number – which makes the consumer more likely to trust the call and pick up. TNS' neighbor spoofing feature analyzes, detects and establishes a reputation for phone numbers and phone calls to help consumers evaluate if a phone call with a familiar area code is legitimate.

TNS Call Guardian correctly identifies spoofed numbers 98% of the time, compared to 64% for nearest competitor based on a recent Mind Commerce study[9].

The combination of deep network integration with our carrier partner networks combined with real-time intelligence of our Call Guardian solution is why TNS is leading in combatting this tactic.

When looking at calls where the calling number and the called number are similar using crowd-source information, the percent of scam-fraud has increased from 19% of the events to 23% of events reported over the first six months of the year.

Neighbor Spoofing based on Crowd Source Data



[9] https://www.vanillaplus.com/2018/08/09/41065-robocall-study-ranks-wireless-carriers-performance-detecting-managing-unwanted-calls/

Industry Solutions to Combat Robocalling

Hardware and Software

Solutions are available as both hardware and software products. Many products are limited to using only on a single medium, such as traditional copper landlines, or mobile phone contracts from a specific mobile phone operator.

Most over-the-top (OTT) software solutions are not integrated with a carrier network and rely on the use of honeypots, 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 techniques is the practice of caller ID spoofing which is prevalent because of the low barrier to entry in the VoIP services market.

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 have the ability to create a user-generated whitelist.[10] Newer devices for landlines can use cloud-based data to resolve the hard-coded blacklist issues and allow you to create your own whitelist/blacklist.

Crowd-sourcing

A more sophisticated model uses crowd-sourcing to build a more comprehensive blacklist of robocall numbers. 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, 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 solutions, require users to provide access to their personal whitelist of genuine contacts, in exchange for access to the larger crowd-sourced database. In 2013, hackers gained access to a Truecaller's database of known genuine numbers, an OTT mobile handset app, highlighting the danger of centralizing this information [11] [12].

[10] https://www.consumerreports.org/cro/magazine/2015/07/robocall-blocker-review/index.htm
[11] https://blog.truecaller.com/2013/07/18/truecaller-statement/
[12] http://www.ehackingnews.com/2013/07/truecaller-database-hacked-by-syrian.html

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 origination of calls 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, as well. On September 30, 2016, the FCC provided clarification that numbers added to the DNO list may be blocked by gateways.[13]

While implementation of DNO is straightforward from a technical perspective, the challenges lie 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 of 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 will play a significant role with respect to blocking and traceback efforts

STIR/SHAKEN

Whereas 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 SIP network, to mitigate caller ID spoofing.

STIR 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 (Secure Telephone Identity Revisited) 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 document developed to provide an implementation profile for service providers implementing STIR.

STIR and SHAKEN use digital certificates, based on common public key cryptography techniques, to ensure the calling number of a telephone call is secure. In simple terms, each telephone service provider obtains their digital certificate from a certificate authority who is trusted by other telephone service providers. The certificate technology enables the called party to verify that the calling number is accurate and has not been spoofed.

STIR may only be used to authenticate and validate origination of the call for U.S. domestic calls and is applicable for SIP-to-SIP calls only. STIR is not applicable for 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 the use of new numbers to avoid detection.

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

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

Real-time Analytics

Once fully deployed, Do-Not-Originate and STIR/SHAKEN will provide crucial layers of protection. Among industry experts engaged in analysis of the issue, 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 call patterns without requiring 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 addresses the constantly changing identities of robocallers. This methodology makes it possible to create an algorithm which can detect call 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, such as whether a telephone number is being used to claim to offer free cruises or is a legitimate call from a bank with a fraud alert related to a credit card.

Enterprise Response to Analytics

TNS has observed a varied response among enterprises to the mitigation techniques we and others have employed. Among the good actors, although, there has been discomfort with this new world in which their calls are being analyzed and characterized, there has been a general willingness to adapt methodologies to conform with the analytics tools' definitions of good behavior.

Branded calling can restore trust to the voice calling experience

As a result, TNS has worked with partners and enterprise allies to develop tools such as Branded Calling, through which a logo and other business information may be displayed. Further, TNS has developed and is in trials with our Reputation Insights product. This solution provides aggregators and enterprises with a lens into their call centers' practices and allows them to understand what will and will not trigger negative reputational scores.

The registration of calling campaigns, for example, will yield positive results, as analytics engines better understand sudden spikes in calling traffic.

Specific to enterprises, one commonly observed trend is enterprises whose main outbound calling numbers are used for multiple purposes 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. A number used for accounts receivable management, for example, should not be used for other purposes, as consumers will invariably provide negative feedback about the number which will impact other outreach efforts via the same number.

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

Conclusions and Recommendations

The FCC continues its exploration of methods to pursue bad actors, including blocking and tracebacks, and seeks the industry's help in its latest public notice 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.

The robocall problem is more complex than it appears on its surface

In addition, analytics providers will be explaining the complex role they play in overlaying context for robocalls that do not involve spoofing and providing the FCC with further insights regarding additional steps that can be taken to address this ongoing problem. The industry will be looking to the FCC for guidance and support as we seek to further differentiate good calls from bad. Further, TNS will seek ways to support the FCC 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 works together 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 layered approach includes the work being done to implement STIR/SHAKEN, the current analytics server role and policy and structure around DNO.

Our goal is that the data and analysis presented in this initial report proves helpful to the industry and robocalling efforts of our partners. TNS will publish this report on a bi-annual basis to help the industry improve its security and detection today and adapt to what we will face in the future.

A layered approach will be most effective in combating robocalls