



governmentattic.org

"Rummaging in the government's attic"

Description of document: Federal Communications Commission (FCC) Reports on Robocalls 2021-2022

Requested date: 23-January-2023

Release date: 28-June-2024

Posted date: 02-December-2024

Source of document: Freedom of Information Act Request
Federal Communications Commission
45 L Street NE
Washington, D.C. 20554
[ArkCase FOIA](#)

The governmentattic.org web site ("the site") is a First Amendment free speech web site and is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.



Federal Communications Commission
Washington, D.C. 20554

June 28, 2024

VIA ELECTRONIC MAIL

Re: Freedom of Information Act Request Control No. FCC-2023-000269

This letter responds to your Freedom of Information Act (FOIA) request, which was received in the FCC's FOIA Office on January 23, 2023.¹ Your request was assigned FCC FOIA Control No. 2023-000269 and referred to the Wireline Competition Bureau (Bureau) for processing. In your FOIA request, you seek the following:

Each memo, white paper, report, study or analysis (or similar documents) regarding progress being made on reducing the extent or number of robocalls. I agree to limit this request to records that are not already published or posted on the FCC website (i.e., have not yet been made public). I agree to limit this request to records that can be located within a 2.5 hour timeframe. I agree to limit this search to the FCC Wireline Office or equivalent.²

The Bureau located 201 pages of records responsive to your request. The records are produced in full without redaction.

Please note that the attached records do not constitute a finding of illegal activity. In the event the FCC identifies illegal conduct, it pursues enforcement actions separate and apart from these records. These records are not in and of themselves determinative as to whether any calls identified may or may not be illegal, or as to whether any parties identified may or may not have violated federal statutes or the Commission's rules or engaged in any unlawful conduct.

In addition to the produced records, we direct you to the record in the Commission's *Advanced Methods to Target and Eliminate Unlawful Robocalls* docket (CG Docket No. 17-59) and the *Call Authentication Trust Anchor* docket (WC Docket

¹ FOIA Control No. 2023-000269 (submitted Jan. 23, 2023)..

² *Id.*

No. 17-97), which may be accessed at <https://www.fcc.gov/edocs>. We also refer you to the following documents:

- Archived reports and recommendations of the North American Numbering Council and its working groups, including those of the Call Authentication Trust Anchor Working Group, available at: <https://www.fcc.gov/about-fcc/advisory-committees/north-american-numbering-council/general/nanc-recommendations>;
- Archived Commission materials relating to robocalls, available at: <https://www.fcc.gov/tags/robocall>;
- The latest TRACED Act Annual Report to Congress, available at: <https://www.fcc.gov/document/fcc-submits-traced-act-annual-report-2023-congress>; and
- A 2021 report on combating illegal robocalls, produced by the Industry Traceback Group, available at: <https://tracebacks.org/wp-content/uploads/2021/08/ITG-Report-Combating-Illegal-Robocalls.pdf>.

We are required by both the FOIA and the Commission's own rules to charge requesters certain fees associated with the costs of searching for, reviewing, and duplicating the sought after information.³ To calculate the appropriate fee, requesters are classified as: (1) commercial use requesters; (2) educational requesters, non-commercial scientific organizations, or representatives of the news media; or (3) all other requesters.⁴

Pursuant to section 0.466(a)(8) of the Commission's rules, you have been classified for fee purposes as falling within category (3), "all other requesters."⁵ As an "all other requester," the Commission assesses charges to recover the full, reasonable direct cost of searching for and reproducing records that are responsive to the request; however, you are entitled to be furnished with the first 100 pages of reproduction and the first two hours of search time without charge under section 0.470(a)(3)(i) of the Commission's rules.⁶ Since the agency's response to your request required two hours of search time and was provided in electronic form, you will not be charged any fees.

If you consider this to be a denial of your FOIA request, you may seek review by filing an application for review with the Office of General Counsel. An application for review must be *received* by the Commission within 90 calendar days of the date of this letter.⁷ You may file an application for review by mailing the application to Federal Communications Commission, Office of General Counsel, 45 L Street NE, Washington, DC

³ See 5 U.S.C. § 552(a)(4)(A); 47 CFR § 0.470.

⁴ 47 CFR § 0.470.

⁵ 47 CFR § 0.466(a)(8).

⁶ 47 CFR § 0.470(a)(3)(i).

⁷ 47 CFR § 0.461(j); 47 CFR § 1.115; 47 CFR § 1.7 (documents are considered filed with the Commission upon their receipt at the location designated by the Commission).

20554, or you may file your application for review electronically by e-mailing it to FOIA-Appeal@fcc.gov. Please caption the envelope (or subject line, if via e-mail) and the application itself as “Review of Freedom of Information Action” and reference FOIA Control Number FCC 2023-000269.

If you would like to discuss this response before filing an application for review to attempt to resolve your dispute without going through the appeals process, you may contact the Commission’s FOIA Public Liaison for assistance at:

FOIA Public Liaison
Federal Communications Commission, Office of the Managing Director
Performance Evaluation and Records Management
45 L Street NE, Washington, DC 20554
FOIA-Public-Liaison@fcc.gov

If you are unable to resolve your FOIA dispute through the Commission’s FOIA Public Liaison, the Office of Government Information Services (OGIS), the Federal FOIA Ombudsman’s office, offers mediation services to help resolve disputes between FOIA requesters and Federal agencies. The contact information for OGIS is:

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Road–OGIS
College Park, MD 20740-6001
202-741-5770
877-684-6448
ogis@nara.gov
<https://www.archives.gov/ogis>

Sincerely,

/s/

Lisa M. Zaina
Chief of Staff and Deputy Bureau Chief
Wireline Competition Bureau

Enclosures

cc: FCC FOIA Office

2021 STI-GA SHAKEN Report

1. Introduction and Background

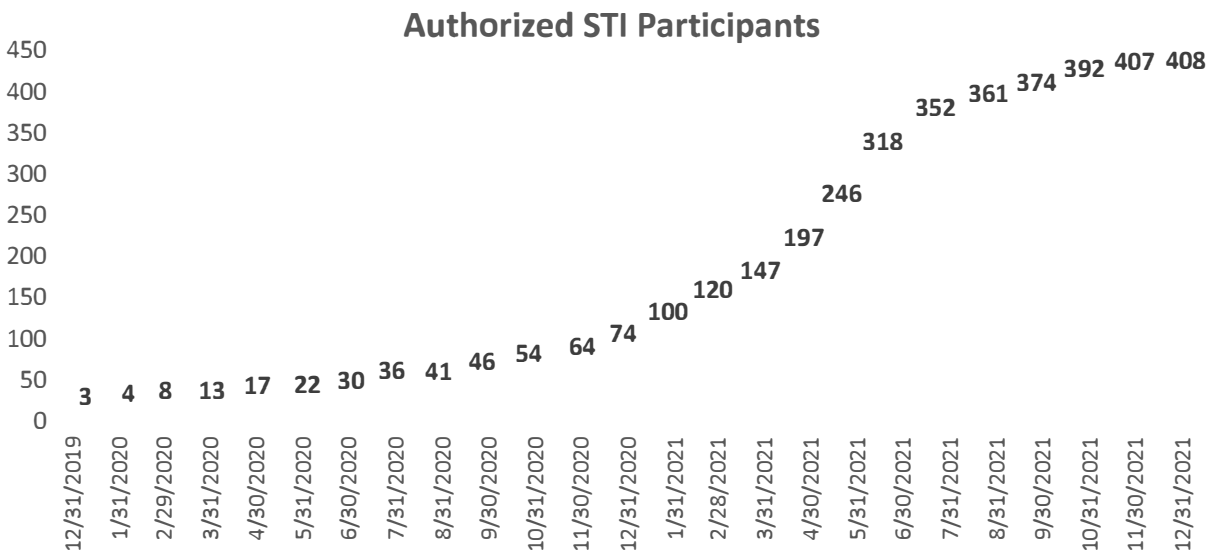
In 2018, the telecommunications industry, under the auspices of the Alliance for Telecommunications Industry Solutions (ATIS), established the Secure Handling of Asserted information using toKENs (SHAKEN) framework; and it organized the Secure Telephone Identity-Governance Authority (STI-GA) as the authority to govern and set policy for use of the framework. Soon thereafter, the STI-GA issued a request for proposal (RFP) for the STI-Policy Administrator (STI-PA), the role required to enforce the STI-GA policy and authorize entities to participate in the SHAKEN ecosystem.

In 2019, the STI-GA completed the RFP process and selected iconectiv as the STI-PA. Additionally, the STI-GA authorized the first four STI-Certification Authorities (STI-CAs) and met the Federal Communications Commission's (FCC's) December 2019 deadline to launch the SHAKEN framework. In 2020, the STI-GA continued its work to ensure the SHAKEN framework was both fully implemented and stable, and created the policies necessary to allow the ecosystem to grow and remain secure.

In 2021, the SHAKEN ecosystem experienced tremendous growth. The year began with 74 service providers (SPs) authorized by the STI-PA and ended with more than 400, more than a fivefold increase in STIR/SHAKEN participation within a single year. Ensuring the framework could grow without sacrificing its dependability and security was an important STI-GA goal.

2. SHAKEN Ecosystem Implementation

As of December 31, 2021, the STI-PA had authorized a total of 408 SPs. The full [list of authorized SPs](#) is posted on the STI-PA website. The chart below exhibits the tremendous pace of growth in the ecosystem during the first half of the year.



A greater number of SPs has allowed the STI-GA to share the costs of the Framework over more participants, generally making it less expensive for SPs to participate in the SHAKEN ecosystem.

The STI-GA Board added another STI-CA to the framework, bringing the total number to ten. Eight of the ten STI-CAs are public in that they serve the entire industry. The [list of public STI-CAs](#) is posted on the STI-PA website. The STI-GA continues to receive applications from prospective STI-CAs indicating the number will continue to grow in 2022.

3. STI-GA Policy

Policy Change Request (PCR): Responsible Organization (Resp Org) Access to Service Provider Code (SPC) tokens

Following finalization of the ATIS Standard on Toll-Free Numbers in the SHAKEN Framework, the STI-GA Board considered a PCR from Somos, the toll-free number administrator. This PCR sought to broaden the SPC token Access Policy to authorize Resp Orgs. A Resp Org is the entity that assigns a toll-free number (TFN) to a customer and is sometimes the only entity that can authenticate a customer's right to use a TFN. Independent Resp Orgs, unlike SPs, neither file a 499A form with the FCC; nor do they hold Operating Company Numbers (OCNs). As such, the STI-GA Board sought equivalent requirements more specific to Resp Orgs. Further changes were made to the SPC token Access Policy to allow for the provision of: 1) a Resp Org ID, a five-digit number, in place of an OCN; and 2) toll-free revenue data, instead of a 499A revenue figure, allowing the STI-PA to determine the appropriate fee level. Resp Org access to SPC tokens was allowed as of October 22, 2021, with the launch of new functionality in the STI-PA systems. Changes to the Revocation Policy were also made to accommodate the inclusion of Resp Orgs into the ecosystem discussed below.

PCR: Optional Use of Delegate Certificates

A second PCR requested the STI-GA Board support the industry's optional use of delegate certificates. A delegate certificate in the SHAKEN context is a digital certificate that allows a non-service provider (non-SP) entity to claim the right to use a specific telephone number, or a group of telephone numbers for outbound calls. A delegate certificate is not the same as an STI certificate and a terminating SP would not use one to validate a call. For example, when an originating SP receives a call from an enterprise, a delegate certificate may be attached to the call in which the enterprise claims the right to use the number shown in the caller ID. The enterprise might do this in an attempt to receive an A-level attestation for that call, even though the telephone number in the caller ID was not assigned to them by the originating SP. Without the delegate certificate claim, the originating SP may not know of the enterprise's right to use the telephone number and may give the call a B-level attestation. If the originating SP has chosen to allow delegate certificates, it may accept the delegate certificate claim as true and give the call level A, the highest level of attestation.

The STI-GA Board approved the necessary changes to the Certificate Policy and the Revocation Policy to allow for the optional use of delegate certificates.

SPC token Access Policy

In May, the STI-GA Board adopted a new SPC token Access Policy allowing SPs to qualify for SPC token Access if they had properly certified in the FCC's Robocall Mitigation Database (RMD). This decision broadened SPC token Access beyond those SPs having direct access to telephone numbers. Having a

current 499A form on file with the FCC and an OCN remained as additional requirements for token access.

The FCC required service providers to file their certifications in the RMD by June 30, 2021. The STI-GA's revised SPC token Access Policy further required service providers that had obtained an SPC token under the previous (direct access to TNs) policy to file in the RMD within 30 days of the FCC deadline, or risk having their token revoked. A list of twenty STI-PA authorized providers was initially found to be non-compliant with this STI-GA requirement. Through notices and direct coordination, each of the providers filed in the RMD and no SPC tokens were revoked.

Certificate Policy (CP) Updates

The Board decisions to allow for use of delegate certificates and Resp Org access to SPC tokens resulted in changes to the CP, the policy that guides STI-CAs in their assignment of the certificates SPs use to sign calls.

One of the most important changes was the issuance of intermediate certificates. An intermediate certificate allows its bearer to assign a lower level of certificate (a delegate certificate) to non-SP entities, such as enterprises. The delegate certificate carries limitations in that it can only be used to authenticate a subset of numbers and it cannot be used to sign a SHAKEN header or to directly provide a level of attestation in a SHAKEN header. The new CP makes the entity assigning such delegate certificates, the one holding the intermediate certificate, ultimately responsible for their use.

Another important change was the institution of an annual letter of attestation. Not to be confused with the level of attestation in a SHAKEN signed call header, the annual attestation is provided by authorized STI-CAs in February of each year. This attestation will provide information on any security issue experienced by an STI-CA during the previous year as well as any major system changes it has made. It is designed to protect the ongoing security of the SHAKEN framework.

The Certificate Policy is an evolving document, and while the Board strives to keep changes to a minimum, it must make edits from time to time to reflect policy decisions or to better protect the SHAKEN framework.

Revocation Policy

Updates to the Revocation Policy were necessary after the addition of Resp Orgs to the ecosystem and the approval of delegate certificate use. With the support of the STI-GA, the FCC issued an NPRM and ultimately an FCC order, establishing a process to hear appeals on STI-GA board decisions on SPC token revocation.¹ While this FCC decision did not change the Revocation Policy, it added another level of appeals for any entity having its SPC token revoked. The FCC Report & Order also largely validated the STI-GA's existing Revocation Policy in this Report & Order.

4. SHAKEN Framework Development

Change Order in Support of Policy Changes

On October 22, 2021, the STI-PA launched changes to its system to support the optional use of delegate certificates and the registration of toll-free Resp Orgs. Both changes were adopted as a result of

¹ See Call Authentication Trust Anchor, WC Docket No. 17-97, FCC Third Report & Order, Adopted August 5, 2021.

requests made through the Board's Policy Change Request process, which opens the ability for non-Board members to have proposed SHAKEN policy changes considered by the Board.

5. Outreach & Education

The primary means of outreach for the STI-GA is its website. This website is kept current with all STI-GA Board policies, including any new policy decisions, through the STI-GA Policy Decisions Binder. Any STI-GA issued media and industry advisories for important announcements are posted and maintained on the website.

The SHAKEN webinar series began in December 2020 and wrapped up with two webinars in January and February, 2021.

The January webinar described the structure of the ecosystem and provided an overview of the process of how service providers can select and work with an STI-CA. It gave service providers direction on the steps to take following registration in the ecosystem and advised them on the proper use and treatment of certificates to ensure the integrity and security of the SHAKEN ecosystem. Finally, it discussed what happens if a certificate is compromised, how that certificate is revoked and how other providers learn of the revocation.

In February 2021, the webinar series concluded with a discussion on how to use the STI certificates for signing calls. This third webinar included a discussion on following the SHAKEN standards in setting the level of attestation on a given call, as well as the role local policy can play in setting that attestation level. There was a discussion on how STIR/SHAKEN influences, but does not determine, what is displayed to the end user receiving a signed call. Finally, the subject of STI-GA revocation of an SP's certificate was discussed along with the best ways for SPs to avoid having their certificate revoked. In total, the three-webinar series had more than 684 registrants, 543 live attendees, and 980 replays thus far.

6. Governance

Funding

At the end of 2020, the Board took steps to ensure funding for the SHAKEN framework in 2021. Large carriers provided the bulk of the funding for 2020 because of the funding uncertainty for the first year which resulted in a very low contribution factor for other participants. In 2021, the Board raised the contribution factor. This raise allowed the Board to ensure full funding of the SHAKEN framework in its first year operating entirely on industry STI-PA fee payments.

The Board-approved 2022 budget is at the same level as its 2021 budget. Due to the growing number of authorized service providers, however, the Board was able to come to agreement on a Funding Policy that substantially lowered 2022 payments for all but the smallest providers. The minimum payment remained at \$825.

With the ecosystem still in a growth mode, the Board will need to adjust the Funding Policy to account for future changes. However, the financial status of the SHAKEN framework in its third year, is solid and fully stabilized.

STI-GA Continuity

In 2021, nine of the twelve Board Director seats were eligible for reappointment. In an industry show of support for the continued work and value of the SHAKEN governance structure, all nine of the Board members with expiring terms sought and were granted reappointment for a second three-year term.

Similarly, the Board first appointed ATIS as the STI-GA in 2018. In 2021, the Board extended the agreement with ATIS as the STI-GA through the end of 2022.

In 2021, nine of the twelve Board Director seats were eligible for reappointment. In an industry show of support for the continued work and value of the SHAKEN governance structure, all nine of the Board members with expiring terms sought and were granted reappointment for a second three-year term.

7. Conclusion

Since the launch of the SHAKEN framework in late 2018, the ecosystem has grown rapidly and is poised for continued growth. As more SPs and Resp Orgs participate in the SHAKEN ecosystem, a greater number of calls will be signed. Increasing the number of verified calls will benefit consumers because SPs will be better able to assess the right of a caller to use the TN that is displayed in the caller ID.

SCAM ROBOCALLS:

TELECOM PROVIDERS PROFIT

June 2022

ABOUT THE NATIONAL CONSUMER LAW CENTER

Since 1969, the nonprofit National Consumer Law Center® (NCLC®) has used its expertise in consumer law and energy policy to work for consumer justice and economic security for low-income and other disadvantaged people in the United States. NCLC's expertise includes policy analysis and advocacy; consumer law and energy publications; litigation; expert witness services; and training and advice for advocates. NCLC works with nonprofit and legal services organizations, private attorneys, policymakers, and federal and state government and courts across the nation to stop exploitative practices, help financially stressed families build and retain wealth, and advance economic fairness.

NCLC.ORG

ABOUT THE ELECTRONIC PRIVACY INFORMATION CENTER

Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C., focused on emerging privacy and technology issues. Since 1994, EPIC has worked at the intersection of policy, advocacy, and litigation. EPIC litigates cases on emerging privacy issues, provides expert advice to policymakers, lawmakers, courts and litigators, and facilitates dialogue between advocates, experts, and decisionmakers. EPIC has worked for strong consumer protections against unwanted and illegal calls through numerous amicus briefs, public comments, and attorney trainings.

EPIC.ORG

© Copyright 2022, National Consumer Law Center, Inc. and Electronic Privacy Information Center. All rights reserved.

ABOUT THE AUTHORS

Margot Saunders is currently Senior Counsel to the National Consumer Law Center (NCLC) after serving as managing attorney of NCLC's Washington, D.C. office from 1991 to 2005. Margot has testified before Congress more than two dozen times regarding a wide range of consumer law issues, including predatory mortgage lending, high cost small loans, payments law, electronic commerce, protecting benefits in bank accounts, privacy issues, and for the past several years--robocalls. She was the lead advocate on the passage of the Home Ownership and Equity Protection Act, the development of the Treasury Rule protecting exempt benefits, and many other initiatives. Margot has served as an expert witness in over 50 consumer credit cases in more than 20 states, providing opinions on predatory lending, electronic benefits, servicing, and credit math issues in individual and class cases. She is a co-author of NCLC's *Consumer Banking and Payments Law*, many articles, and a contributor to numerous other manuals. Prior to joining NCLC, she was the consumer law specialist for North Carolina Legal Services. In 1991, Margot was the second recipient of the Vern Countryman Award. She is a graduate of Brandeis University and the University of North Carolina School of Law.

Chris Frascella is a Law Fellow in Telephone Subscriber Privacy at the Electronic Privacy Information Center (EPIC), where his work focuses primarily on robocalls and data brokers. Chris has contributed to multiple amicus briefs explaining the technology and policy underlying the Telephone Consumer Protection Act (TCPA), and has submitted comments to state and federal agencies on topics including robocalls, SIM swapping, prison phone surveillance, fraudulent emergency data access requests, broadband privacy, and app-based payment platforms. As a law student, his internship experiences included the Federal Trade Commission's Bureau of Consumer Protection, the Office of Consumer Protection within the DC Office of the Attorney General, the Bureau of Internet and Technology (BIT) within the NY Attorney General's Office, the Administrative Conference of the United States (ACUS), and the Office of Privacy and Civil Liberties within the U.S. DOJ. Prior to law school, Chris worked for nearly a decade in digital marketing for software startups. He is a graduate of the George Washington University Law School, American University, and Fordham University.

ACKNOWLEDGEMENTS

The authors would like to thank NCLC Deputy Director Carolyn Carter and EPIC Senior Counsel Megan Iorio for their invaluable analysis, advice, and reviews; Maggie Westberg, NCLC's Research Assistant for compiling the information in Appendix 2, Alinnah Qiao, Executive Assistant at EPIC for proofreading assistance with Appendix 2, and Emily Caplan for essential citation checks and corrections. The authors would also like to extend their special thanks for the creativity and expertise shared by David Frankel, CEO of ZipDX, and Ted Hobson, an attorney with the Consumer Assistance Program in the Vermont Attorney General's Office (whose contributions were his own personal opinions and are not necessarily shared by the Vermont Attorney General). Additionally, we very much appreciate the illustrative data provided by Mike Rudolph, CTO of YouMail. We appreciate the indispensable assistance of NCLC's communications and operations team, Michelle Bates Deakin, Stephen Rouzer, and Moussou N'Diaye, and we'd like to thank Julie Gallagher for layout and design assistance. The views expressed in this report are solely those of NCLC and EPIC and the authors.

SCAM ROBOCALLS:

TELECOM PROVIDERS PROFIT

TABLE OF CONTENTS

EXECUTIVE SUMMARY	3
<i>What needs to be done to stop the fraudulent calls.</i>	5
I. AMERICANS ARE LOSING BILLIONS OF DOLLARS EVERY YEAR FROM SCAM ROBOCALLS.	6
<i>A. There are billions of scam robocalls every year.</i>	6
<i>B. Scam robocalls cost American subscribers almost \$30 billion in 2021.</i>	8
II. SCAM TEXTS ARE INCREASING.	10
III. HOW DID THE U.S. TELEPHONE SYSTEM BECOME SUCH A MESS?	11
<i>A. Providers' choices determine whether scam calls reach subscribers.</i>	11
<i>B. U.S. providers are complicit in routing illegal robocalls originating in the U.S. and abroad.</i>	12
<i>C. Tracebacks reconstruct the call path of illegal robocalls.</i>	14
<i>D. Providers are aware of their role in delivering illegal calls.</i>	16
<i>E. Providers have a system to filter out some spam texts, but it is insufficient.</i>	18
IV. THE U.S. GOVERNMENT HAS NOT BEEN ABLE TO STOP THE SCAM CALLS.	19
<i>A. The Federal Communications Commission's (FCC's) approach to regulating robocalls has not solved the problem.</i>	19
<i>B. The Federal Trade Commission's (FTC's) enforcement of the Telemarketing Sales Rule (TSR) is unlikely to stop the illegal calls.</i>	25
V. THE FCC CAN STOP MOST SCAM ROBOCALLS AND ILLEGAL TEXTS—HERE IS HOW.	26
ENDNOTES	31

APPENDICES

APPENDIX 1	Other Invasive Robocalls	46
APPENDIX 2	Scam Robocalls in the States	50

TABLES

TABLE 1	Total Annual Scam Robocalls 2018 Through 2021	6
TABLE 2	Rate of Complaints to FTC About Scam Calls and Scam Texts from 2017 to 2021	8
TABLE 3	Number of Americans that Lost Money to Scam Calls	9
TABLE 4	Total Losses from Scam Calls	9
TABLE 5	Call Path from Foreign Originating Provider to Terminating Provider	12
TABLE 6	Comparing Legal Robocalls to <i>Illegal</i> Robocalls	17

EXECUTIVE SUMMARY

Every month, more than one billion scam robocalls designed to steal money from unsuspecting telephone subscribers are made possible because providers—typically small, pop-up VoIP telephone providers—transmit these calls through to our telephones. Every answered scam robocall pays money to those providers, as well as to every telephone service provider in the call path.

Even when these providers are told—sometimes repeatedly—that they are transmitting fraudulent calls, they keep doing it, because they are making money from these calls. And even when they are caught and told to stop, they are not criminally prosecuted, and the fines that are levied are rarely collected. FCC Commissioner Geoffrey Starks has noted this counterproductive dynamic regarding robocalls: “[I]llegal robocalls will continue so long as those initiating and facilitating them can get away with and profit from it.”

This report explains the depth of the problem, the reasons for the problem, and how the Federal Communications Commission has responded. We recommend several simple strategies that would stop most, if not all, of these fraudulent robocalls.

Problem: Every month well over one billion scam robocalls—calls to defraud telephone subscribers—are made to American telephones. This is more than 33 million scam robocalls every day. Criminals make these calls to scare or trick Americans into turning over hundreds or even thousands of dollars.

Typical frauds include calls scaring seniors into believing that unless they turn over thousands of dollars they will lose access to their [Social Security](#) or [Medicare benefits](#); threats to immigrants that if they don't pay the caller they will be deported; and calls in which the recipient is tricked into believing they have been refunded too much money by [Amazon](#) or [Apple](#), requesting that the excess be returned. Other typical scams include selling phony [health insurance](#), calls purporting to be from the [IRS](#), [student loan scams](#), threats of arrest, debt reduction scams, and scam tele-marketing calls (such as the ubiquitous [auto warranty call](#)). These scam robocalls are in addition to the annoying, but not necessarily illegal, calls from debt collectors, people taking surveys, and charities summarized in Appendix 1. Scam texts are also increasing, and are similarly effective in stealing money from consumers.

Look for the  to listen to recordings of real robocalls attempting to scam consumers.

Last year almost **60 million Americans** lost over **\$29 billion** to these scam callers. More than one million complaints were made to the FTC about scams from calls and texts.

Illegal calls impair the value and efficiency of the U.S. telephone system. The problem has become so pervasive that 70% of Americans do not answer calls from numbers they do not recognize. This increases costs for health care providers, small and large businesses, and their call recipients, who miss or incur delays in receiving time-critical communications for fear of answering a robocaller. These unwanted calls are also a prime reason that many landline subscribers are dropping their landline subscriptions.

Causes. One cause of this current mess is the deregulation of the American telephone system, which has deregulated the call path for long distance calls. Rather than a single telephone company transferring the calls directly from the caller to the called party, multiple providers transmit calls from the caller to the called party. Each transfer of the calls from one provider to the next involves a separate agreement between the providers, which determines the price the upstream provider will pay the next downstream provider to transfer the calls. This process also allows downstream providers to refuse to take calls from upstream providers if they do not like the price offered for the transmittal, or if they deem the calls potentially illegal—and thus too costly.

Another cause is the development of VoIP (a technology that accesses the telephone network through the internet), which allows callers to reach U.S. telephone subscribers with minimal expense. Many small VoIP providers are honest businesses, but a few are complicit in facilitating the fraudulent calls. Unlike large, facilities-based telephone providers, small VoIP providers often set up service in temporary quarters or their home and offer their services through online advertisements. Once caught facilitating scam calls, they need only change their name to pop up under a different business identity and continue operations.

The telecom industry continues to transmit tens of billions of illegal calls each year because every answered call provides revenue for the transmitting voice service providers. Each provider in the call path makes a fraction of a cent for every answered call that it transmits. While the terminating providers strive to block illegal calls, the complicit originating provider and some intermediate providers find it profitable to continue processing these calls. Providers can choose not to accept fraudulent robocalls from upstream providers, but they need to be incentivized to reject these calls.

Government Response. Congress passed the Telephone Consumer Protection Act (TCPA) in 1991 to limit unwanted calls by requiring that callers have prior express consent for autodialed calls to cell phones and prerecorded calls to cell phones and residential lines. In 2019, Congress passed the TRACED Act, requiring—among other things—that the FCC issue regulations to authenticate the caller IDs shown on telephone calls (known in the industry as STIR/SHAKEN), establish a method to trace the sources of illegal calls by naming

an “Industry Traceback Group” (ITG), and require providers to respond to ITG requests for information about illegal calls.

The FCC has initiated regulatory efforts and enforcement actions aimed at controlling these illegal calls. Yet, every month, well over a billion scam robocalls continue to ring on the telephones of U.S. subscribers.

The problem is that applying the STIR/SHAKEN methodology requires only that originating providers apply a certification indicating how confident they are that the caller ID displayed in the calls is correct. It does not cause the scam calls to stop. And the FCC’s pending regulatory efforts would continue to require only that providers have procedures in place to mitigate illegal robocalls, with no meaningful and enforceable requirement that these procedures actually be effective.

What Needs to Be Done to Stop the Fraudulent Calls.

Providers choose whether to accept calls from upstream providers. These decisions are now generally based only on the prices upstream providers pay for processing their calls down the call path toward the recipient. This dynamic is key: the rules governing the process used by providers must provide strong incentives for all providers in the call path (from caller to called party) to *refuse to transmit calls likely to be illegal*.

There are multiple tools available to providers that inform them about the potential illegality of the calls coming their way. These include information from tracebacks done by the Industry Traceback Group about which providers have transmitted illegal calls, examination of the provider’s call detail records, and analysis of the content of the calls (available through various industry service providers).

If these crimes were occurring in the physical world, rather than over the telephone and internet, law enforcement would not hesitate to arrest the thieves and their helpers to stop them from stealing. The FCC should provide the same level of protection to American telephone subscribers.

We propose three principles to stop the criminal robocalls:

1. All providers in the call path should have an affirmative obligation to engage in effective mitigation against illegal robocalls.
2. Providers who knew or should have known that they were transmitting illegal robocalls should face clear financial consequences.
3. Law enforcement, telephone service providers, victims of scam calls, legal robocallers, and the general public should have access to all available information about the sources of the illegal robocalls and their complicit providers.

Our five specific proposals to accomplish these principles are included on [page 26](#).

I. AMERICANS ARE LOSING *BILLIONS* OF DOLLARS EVERY YEAR FROM SCAM ROBOCALLS.

Every call we receive that uses a prerecorded or artificial voice is a “robocall.”¹ Not every robocall is annoying—we appreciate the reminders from our doctor’s office or the warning from the airline that our flight is late. But unwanted robocalls are invasive and aggravating. And some are outright attempts to defraud us.

Robocalls, whether made to cell phones or to landlines, are governed by the Telephone Consumer Protection Act (TCPA) passed by Congress in 1991.² Most are legal only if the recipient has provided *prior express consent* for the call or if the Federal Communications Commission (FCC) has exempted the particular type of call from this requirement.³

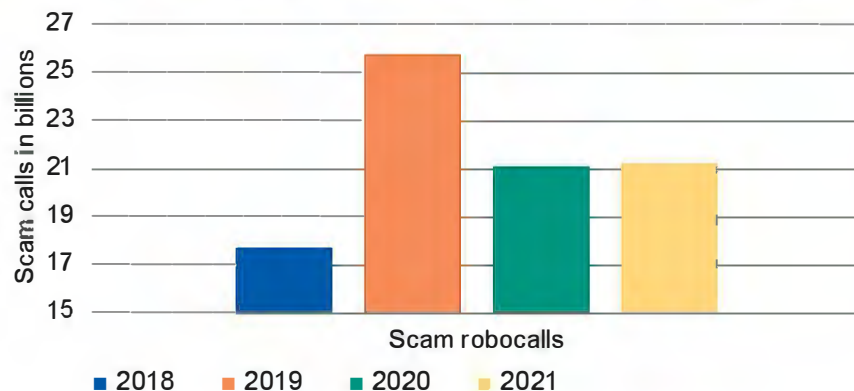
This report is about robocalls that perpetrate frauds against telephone subscribers—scam robocalls. The number of these scam robocalls continues to escalate, and Americans are losing an increasing amount of money to scam robocalls.⁴

A. *There are billions of scam robocalls every year.*

More than **one billion scam robocalls**⁵ are made to American telephones every month, all seeking to defraud American telephone subscribers. This is over 33 million scam robocalls every single day. (See Appendix 2 for illustrations of scam robocalls in each state.)

TABLE 1

Total Annual Scam Robocalls 2018 Through 2021⁶



Scam robocalls assault seniors, immigrants, people with disabilities, student loan borrowers, and any recipient of the call. The top 1,000 scam robocall campaigns are responsible for a large percentage of scam robocalls.⁷ Examples of typical robocall scams include:

Scams against seniors. In a standard senior scam scenario, a **prerecorded call** 🗣️ from someone claiming to be from the Social Security Administration is answered by a senior citizen. This happened recently to a retired Virginia woman in her 60s caring for her disabled son; she received a robocall purportedly from the Social Security Administration with a message that federal drug agents had found her information connected to a car transporting cocaine. Alarmed, she responded, and then fell victim to the scammer, who swindled her out of most of her nearly \$445,000 in savings. She now lives on her son's disability payments and her Social Security.⁸

This type of scam is all too frequent. Hundreds of thousands of calls are made every month to seniors threatening arrest or suspension of benefits for a fictitious problem with Social Security benefits.⁹ Complaints made by seniors to the FTC about scams in general are increasing. Seniors reported over \$1 billion in fraud losses in 2021.¹⁰



Scams against immigrants. One horrific scam against immigrants starts with robocalls in Mandarin to Chinese immigrants. The message purports to be from the Chinese Consulate, and the victims are told, "There is an important document that needs to be picked up; it may affect your status in the U.S.; press a button to speak with a specialist." When the immigrant presses the button, the connection is made to a live scammer. In one example of this scam, a 65-year-old Chinese immigrant in New York was scammed out of \$1.3 million after receiving Chinese-language robocalls claiming that she was being investigated for financial crimes in China.¹¹

Scams against people with disabilities. Every month, there are millions of **scam calls** 🗣️ offering fake assistance applying for Social Security disability benefits where the true goal of these calls is to gain the recipient's personal information to steal their identity.¹²

Scams against student loan borrowers. Typically, these **scam calls** 🗣️ attempt to scare the recipient into answering the call with the threat of a collection action or termination of a payment suspension. The goal is to solicit personal information to facilitate identity theft.¹³

Scams against anyone who answers the telephone. Leading scam robocalls that are not specifically targeted include **vehicle warranty** 🗣️,¹⁴ **Medicare** 🗣️,¹⁵ **health insurance** 🗣️,¹⁶ and **bill reduction** 🗣️ scams.¹⁷ Other common types of scam robocalls are government imposter scams

Look for the 🗣️ to listen to recordings of real robocalls attempting to scam consumers.

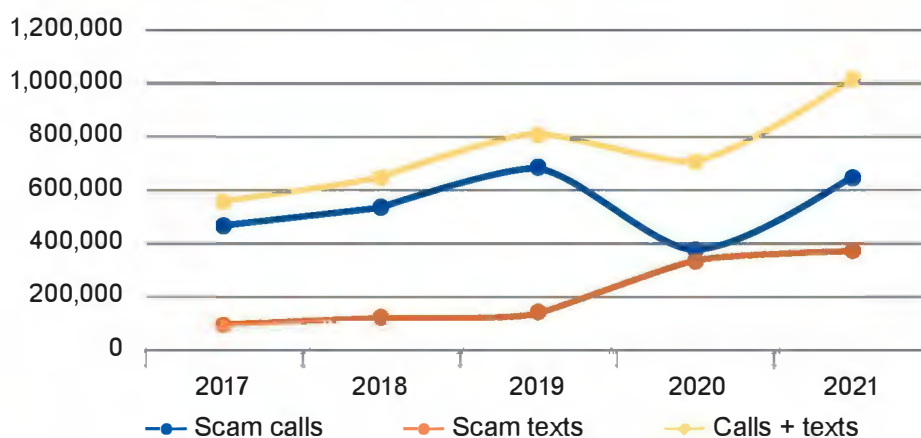
(e.g., calls purporting to be from the IRS ¹⁸) and calls impersonating a business such as Amazon ¹⁹. For each of these types of scam robocalls, tens of thousands (sometimes hundreds of thousands) of calls are made to American telephone subscribers every month.²⁰ More stories about these scam calls are included in the state pages in Appendix 2.

Scam callers typically use disguised caller IDs to hide the real number used to make the call and their identity.²¹ Often the caller spoofs the telephone number of a trusted source, such as the Social Security Administration, the IRS, or a local hospital, or uses a number that makes it appear that the caller is someone in the called party’s neighborhood.²² Scam callers increasingly “rent” a large block of telephone numbers, sometimes changing to a different number for each call, in order to make it harder to identify the calls as scam calls or block them.²³

The Federal Trade Commission (FTC) reported 644,048 complaints of fraud attempted through a phone call and another 377,840 about texts to cell phones, totaling over 1 million. This was an increase of 37% from the previous year.²⁴ While not all of the complaints were about scam robocalls (some may have been about live calls), applying Truecaller’s estimate that 60% of scam calls are robocalls,²⁵ that means that in 2021 there were more than 386,500 complaints about scam robocalls.²⁶

TABLE 2

Rate of Complaints to FTC About Scam Calls and Scam Texts from 2017 to 2021²⁷

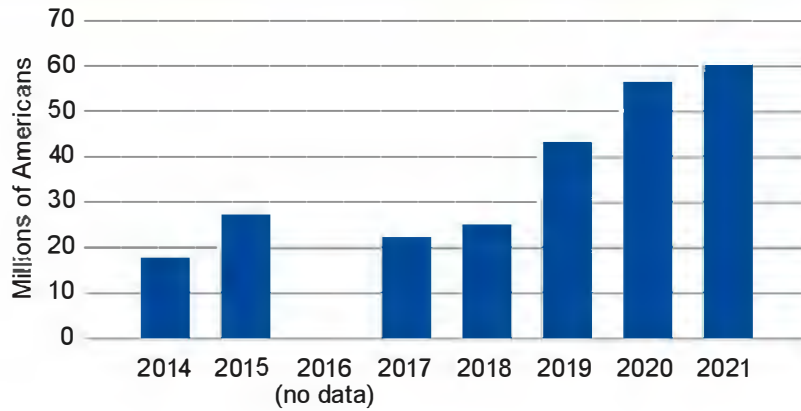


B. Scam robocalls cost American subscribers almost \$30 billion in 2021.

Harris Poll surveys show that **59.4 million Americans were victims of fraud through calls or texts in the 12-month period ending in June 2021.**²⁸

TABLE 3

Number of Americans that Lost Money to Scam Calls²⁹



This data shows that U.S. telephone subscribers had an estimated **\$29.8 billion stolen through scam calls in the 12 months before June 2021**, an increase of over 50% in just one year.³⁰ Even the FTC’s data, based just on losses affirmatively reported by consumers, documents that \$692 million was stolen in 2021 through **scam calls**.³¹ The FTC reports the median amount lost by each victim to scam calls was \$1,200 in 2021.³² And, the FTC found that those over 80 years of age lost an average of \$1,500 to scams in 2021.³³ In a special report on scams against seniors completed in 2021, the FTC found that for consumers over age 60, the median loss from scam calls was \$1,800, and for consumers over age 80, the median loss from scam calls was nearly twice as high at \$3,000.³⁴

TABLE 4

Total Losses from Scam Calls³⁵

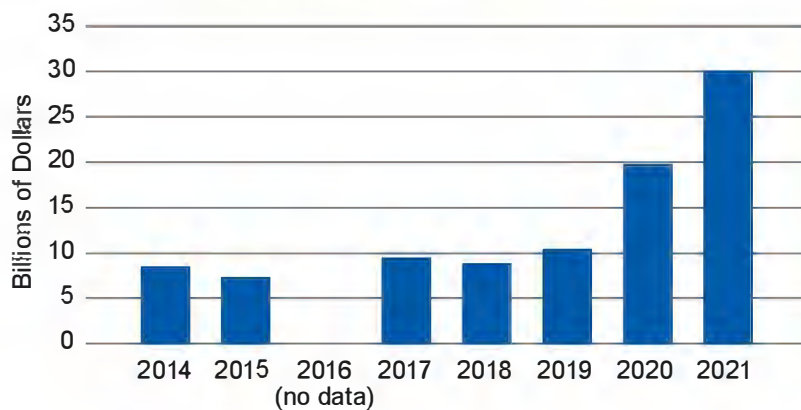


Table 4 illustrates the dramatic growth in losses suffered by the *direct victims* of fraudulent calls. However, defrauded American telephone subscribers are not the only losers from illegal calls. Even consumers who are not duped by these calls

suffer costs in the form of wasted time and nuisance—that the FCC estimates amount to at least \$3 billion annually.³⁶

Robocalls are a major cause of the degradation of the U.S. telephone network. The problem has become so pervasive that 70% of Americans do not answer calls from numbers they do not recognize.³⁷ One hospital reported persistent inability to reach patients due to call screening.³⁸ Contact tracing efforts during the first months of the COVID-19 pandemic were also severely impacted by phone subscribers refusing to pick up because they expected a call from an unknown number to be a waste of their time.³⁹ Unwanted calls are also a prime reason why many landline subscribers are dropping their landline subscriptions.⁴⁰

II. SCAM TEXTS ARE INCREASING.

Scammers are increasingly moving towards texts as a way to avoid the protections erected against illegal robocalls.⁴¹ To avoid detection, text scammers are using the same methods callers use to spoof telephone numbers.⁴²

In a typical text scam, a scammer sends an alluring text message inviting the recipient to click on a link, which initiates a fraudulent transaction with the scammer.⁴³ Fraudulent texts take many forms, including messages impersonating package delivery companies or appearing to advertise real items for sale.⁴⁴

The number of complaints to the FTC about scam texts rose to 377,840 in 2021, up by over 12% in one year, and by a whopping 315% since 2017.⁴⁵ (This is illustrated in Table 2, *supra*.) Similarly, complaints made in 2021 to the FCC about unwanted texts (many of which are likely to have been scams) rose by over 143% between 2017 and 2021.⁴⁶

The most unfortunate consequence of the rise in spam texts is the dramatic increase in *direct consumer losses from scams and frauds perpetrated by those texts*. In 2021, victims reported losses of \$131 million, a 254% increase from 2017.⁴⁷ The actual losses to American consumers are likely even greater than this figure, as only a small percentage of fraud is reported.

Texts are treated as “calls” under the Telephone Consumer Protection Act (TCPA).⁴⁸ As a result, a text can be sent to a cell phone using an “automated telephone dialing system” (ATDS) only with the recipient’s prior express consent.⁴⁹ In addition, whether or not it is autodialed, a text that includes a telemarketing message cannot legally be sent to a cell phone that is considered a residential line and is registered on the National Do Not Call Registry.⁵⁰ But some courts interpret the U.S. Supreme Court’s 2021 decision in *Facebook, Inc.*

*v. Duguid*⁵¹ in such a narrow way that the ATDS definition does not apply to the autodialers used today to send mass texts.⁵² And the Do Not Call registry applies only to residential lines, and only to messages “for the purpose of encouraging the purchase or rental of, or investment in, property, goods, or services. . . .”⁵³ Moreover, the entities sending scam texts are typically located overseas, are adept at evading identification, and generally ignore all aspects of the FCC’s rules. As a result, the TCPA’s restrictions provide little effective protection from scam texts for American consumers.

III. HOW DID THE U.S. TELEPHONE SYSTEM BECOME SUCH A MESS?

Voice service providers determine whether scam calls reach consumers’ phones. Call traffic of any kind (legal or illegal) translates into profit for smaller providers. Even when scam calls are traced back through their networks, or when they are notified of illegal call traffic by other means (such as their own analytics tools or other protocols they certify are part of their robocall mitigation program), these providers continue to let these calls through, prioritizing their own revenue because their stake in the harm to consumers is negligible.

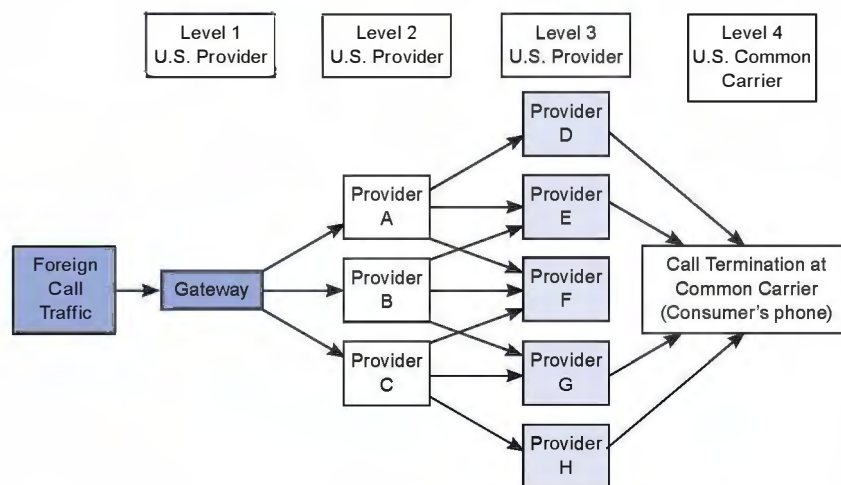
A. Providers’ choices determine whether scam calls reach subscribers.

Decades ago, consumers paid as much as \$0.25 per minute for local calls,⁵⁴ with increased rates for long distance calls.⁵⁵ Today, because “wholesale rates to U.S. mobile phones are less than a penny per minute and accessible virtually worldwide,”⁵⁶ consumers pay much lower telephone costs for local and long distance calling.

The reduction in the cost of long distance calling is a function of changes in how long distance calls are routed from the caller to the called party. Rather than a single telephone company transferring the calls directly from the caller to the called party, calls now pass through multiple providers. Calls enter the U.S. telecommunications network through an “originating provider,” which provides service directly to callers,⁵⁷ or through a “gateway provider,” a U.S. telecommunications company that receives a call that originates overseas.⁵⁸ This provider passes the call downstream to an “intermediate” provider,⁵⁹ which then chooses, in turn, the next intermediate provider that will transmit the call down the call path toward the recipient. At the end of the call path, often after many hops from one intermediate provider to another, the call reaches the “terminating provider,” which routes the call to the called party.

All of these transfers are made pursuant to agreements between the providers, setting forth the price the upstream provider will pay the next downstream provider for accepting and transmitting the calls. Each carrier in the call path generally seeks “least cost routing,”⁶⁰ thus spurring competition to offer lower rates per call. This process also allows downstream providers to refuse to take calls from upstream providers if they do not like the price offered for the transmittal, or if they deem the calls potentially illegal—and thus too costly.

TABLE 5
**Call Path from Foreign Originating Provider
 to Terminating Provider⁶¹**



This process allows telephone users to receive the benefits of the increased competition among the providers. But letting market dynamics determine a call’s path also creates new ways for bad actors to process scam calls to victims. A single successful fraud resulting from one call out of half a million robocalls more than covers the slight expense of the entire high-volume scam robocall campaign.⁶²

B. U.S. providers are complicit in routing illegal robocalls originating in the U.S. and abroad.

Approximately half of the callers making government and business imposter calls are located overseas. To reach American telephones, the calls must be transmitted through a gateway provider based in the U.S.⁶³ Typically, these providers, the originating providers that service fraudulent robocallers, and the first few intermediate providers for these calls, are small companies using VoIP (Voice over Internet Protocol) services.⁶⁴

“In the course of this investigation, I learned that with little more than off-the-shelf VoIP technology, an autodialer, and a business relationship with a gateway carrier, any individual or entity with a broadband internet connection can introduce unlimited numbers of robocalls into the U.S. telephone system from any location in the world.”—Marcy Ralston, Special Agent, Social Security Administration, Office of the Inspector General⁶⁵

VoIP is a technology that accesses the telephone network through the internet, and is commonly used by many large telecommunications providers in place of traditional landlines to provide service to residential and business customers. Often, the telephone service is paired with internet access and cable television service.

The VoIP providers that process the illegal robocalls are generally small, often simply one or two individuals with minimal investment or technical expertise who have set up a service in their home or other temporary quarters and offer services through online advertisements.⁶⁶ These small VoIP providers are often called “nomadic” VoIP services⁶⁷ to distinguish them from the much larger “fixed interconnected VoIP service” providers that tend to be fairly large companies such as AT&T⁶⁸ or Xfinity,⁶⁹ which own their own equipment and provide fixed telephone numbers with service to landline telephone customers.⁷⁰

While some small VoIP providers strive to allow only law-abiding callers into the network, some of them deliberately turn a blind eye to patently illegal traffic.⁷¹ These complicit VoIP providers send their calls to larger voice service providers (VSPs), who in turn transmit the calls to the terminating providers.

As explained by the Vermont Attorney General in a recently filed complaint against a small VoIP provider, a “fraudulent robocall now most frequently ‘hops’ from a foreign entity to a domestic voice service provider (as the U.S. point of entry), then on through multiple domestic intermediary domestic providers to a large domestic carrier—such as Verizon Wireless or AT&T—that ultimately terminates the call with connection to an actual phone.”⁷²

The transmission of illegal, fraudulent robocalls typically works like this:

- First, a foreign originating provider transmits an illegal robocall campaign and sends it over the internet to a U.S. based VoIP service—the gateway provider.⁷³
- Alternatively, a U.S. originating provider originates the call and sends it to a different U.S. based provider. Sometimes, however, calls may flow from the U.S. to foreign providers and then back into the U.S. in an attempt to hide the identity of the real originating provider.⁷⁴
- Typically, robocalls travel from smaller U.S. providers to larger U.S. providers, and then on to the terminating provider that delivers the call to the subscriber.⁷⁵

- In each transition from one provider to the next, the sending provider is charged something for each call by the receiving provider.⁷⁶

As the calls move from originating or gateway provider to the first intermediate provider, and then on down the line to subsequent intermediate providers, they are mixed with calls from other providers. Because some intermediate providers accept both illegal traffic and legal calls (both automated and conversational traffic), calls from different sources get blended together as traffic passes from provider to provider, making identification of fraudulent calls most difficult for terminating *providers furthest removed from the source of the scam calls*.

Fraudulent callers also spoof caller IDs to make detection more difficult.

A cottage industry has developed for VoIP providers who offer “dialer traffic” to facilitate both legal automated calls as well as the fraudulent calls plaguing American telephones.⁷⁷ The legal calls provide cover for the illegal calls. Some of the VoIP providers involved in these calls explicitly present their services as especially valuable for callers making illegal calls who are seeking to avoid the efforts of the downstream providers who try to protect their subscribers from mass scam robocall campaigns.⁷⁸ For example, some advertise and provide a service that allows their robocalling customers to use a different caller ID for each robocall,⁷⁹ as a way to avoid the blocking and labeling efforts used by the downstream service providers striving to protect their customers from these scam calls.⁸⁰ By contrast, legitimate telemarketing robocallers tend to rely on consistent use of a relatively small set of caller IDs for outbound call campaigns to track the effectiveness of their efforts.⁸¹

Originating providers, gateway providers, and at least the first intermediate provider that receives the calls from the originating or gateway providers should be fully aware of the nature of the fraudulent calls being transmitted, if they paid any attention. As explained in the next two subsections, multiple tools are already available to providers that try to avoid transmitting fraudulent robocalls. Without the complicit gateway and intermediate voice service providers based in the U.S., few foreign fraudulent robocalls would ever reach American telephones.⁸²

C. Tracebacks reconstruct the call path of illegal robocalls.

To find the criminal callers and their complicit providers, the TRACED Act required the FCC to select a group to conduct tracebacks of suspected unlawful robocalls.⁸³ The FCC selected USTelecom,⁸⁴ a trade association for telephone companies and providers of broadband services, to be the Industry Traceback Group (ITG).⁸⁵

Tracebacks work like this:

- Using a secure portal, the ITG contacts the terminating provider that delivered the unlawful call to the consumer and gives that provider (1) the time and date of the call, (2) the calling number, (3) the called number, (4) the specific nature and content of the illegal robocall in question, and (5) the likely laws violated by the call.⁸⁶
- ITG then asks that terminating provider to identify the upstream voice service provider that transmitted the call to it. Once the carrier identifies which upstream provider routed the call to it, ITG contacts *that* upstream provider using a database tool. As it did with the previous carrier, ITG provides notice of the nature and content of the illegal robocall, including a link to a recording of the call, and asks the upstream provider to identify which further upstream provider routed the call to it.⁸⁷
- In turn, each voice service provider in the call path provides the ITG with the identity of the upstream voice service provider from whom it received the suspicious traffic and enters the information into the portal.⁸⁸ The process continues until the originating voice service provider is identified or a dead end is reached.⁸⁹

As the Vermont Attorney General explained in a recent complaint filed against a complicit gateway provider:

By this method, ITG “asks” its way up the call-path, identifying each of the domestic . . . [voice service providers] involved in facilitating the illegal robocall in question, and [putting] each on notice of the nature and content of that call. At some point in most tracebacks of government or business imposter fraud, a domestic [voice service provider] reports to ITG that it received the call from a foreign customer. Thus, ITG—under FCC authority—identifies the . . . [voice service provider] that served as the U.S. point of entry to the illegal robocall.⁹⁰

Each traceback is of a single telephone call. But robocalls, by their very nature, are never made by themselves. Each robocall is indicative of thousands of similar—usually identical—calls, with the only difference being the recipient of each call. As a result, when the ITG identifies which U.S. voice service provider routed a single illegal robocall into the U.S. from abroad, the ITG has identified the provider that delivered a torrent of illegal calls to American telephones.

The ITG traced 2,500 calls determined to be illegal in 2020⁹¹ and 2,900 calls in 2021.⁹² The ITG traceback process informs the ITG and the FCC of the service providers that are the sources of these illegal calls: either the U.S. based originating providers or the gateway providers.

The traceback process also informs each of the voice service providers in the call path, including all the intermediary providers, that a traceback through that provider's system is being conducted, and that the traceback relates to an illegal robocall. As explained in the complaints filed by both the North Carolina and Vermont Attorneys General, the ITG provides a notice to each provider in the call path explaining that they have transmitted "suspected and known fraudulent and/or illegal robocalls."⁹³ The ITG usually sends to each provider a link to an audio recording of the illegal robocall.⁹⁴

D. Providers are aware of their role in delivering illegal calls.

Tracebacks. The providers that are complicit in transmitting illegal calls are well aware of what they are doing. They know that the calls are illegal because they have received multiple traceback requests. With each traceback request,⁹⁵ they are given a notice from the ITG that they are transmitting suspicious calls.⁹⁶ **So, even if the providers did not know before they received the traceback request from the ITG that the calls transmitted over their networks were illegal, the providers are fully aware once the traceback requests start arriving.**

Intermediate providers are also complicit if they continue transmitting calls from gateway or originating providers after receiving notices that calls they received from those providers were the subject of multiple traceback requests. For example:

- In a case against gateway provider Startel brought by the Indiana Attorney General, a defendant downstream intermediate provider, Piratel, received four traceback requests in three weeks about calls it accepted from Startel.⁹⁷
- In a case brought against Articul8, another intermediate provider, by the North Carolina Attorney General, the defendant had received 49 traceback requests.⁹⁸

Behavioral Analytics. Providers need not wait to receive a traceback request from the ITG to know that the calls they are transmitting are illegal. The providers have specific tools to evaluate on a granular level which robocalls are illegal. Every provider maintains Call Detail Records (CDRs) for each and every call. (It is through the CDRs that the providers are paid for their calls and the traceback process is conducted.) The CDRs include the duration, source number, and name of the upstream provider for each call. Through the CDRs, providers can distinguish between legal and illegal robocalls by examining the percentage of calls answered, the ratio of different caller ID information displayed (referred to as Automated Numbering Information, or ANI) to the number of total calls, the average duration of calls, and the percentage of calls of less than one minute.⁹⁹ These behaviors will show clear indications of fraud.

TABLE 6
Comparing Legal Robocalls to *Illegal* Robocalls¹⁰⁰

LEGAL ROBOCALLS	ILLEGAL ROBOCALLS
Relatively high percentage of calls are answered	Low percentage of calls are answered
Legitimate telemarketer typically uses only a single caller ID for the entire telemarketing campaign or demographic. (This allows callers to track their calls)	Spoofer caller IDs, with caller ID-to-called-number ratios often fewer than 2 (meaning that each caller ID is used for 2 or fewer calls)
	Almost all calls are short duration, <ul style="list-style-type: none"> ■ averaging less than 20 seconds (because the called party hangs up or sends to voicemail) ■ 99% or more of calls last less than a minute ■ Fewer than 1% of calls last more than 2 minutes

The recently filed case by the North Carolina Attorney General against provider Articul8 provides a concrete example of how these metrics can be used to determine illegal calls. According to the complaint, in a single day Articul8 routed through a downstream (intermediate) provider over 17 million calls, more than 70% of which were not answered. Of the 4.4 million calls that were answered the average duration was 11 seconds. The call-per-ANI ratio was 1.08, meaning nearly each of the more than four million calls seemed to come from a distinct (illegally spoofed) number.¹⁰¹

With these hallmarks of fraud, the information in the CDRs is clear indication that the calls are illegal robocalls. And reviews of their own CDRs inform responsible providers of the type of traffic they are transmitting.¹⁰² Indeed, responsible providers review their CDRs regularly to ensure that they are not transmitting illegal calls and to terminate relationships with upstream providers whose calls bear indications of fraud.¹⁰³

However, as CDRs are also proof of illegal traffic, some providers seek to eliminate that proof by destroying their CDRs and those of their downstream providers. Indeed, in its recent complaint, the Vermont Attorney General alleges that the defendant was “deliberately” destroying these records.¹⁰⁴

Content Analytics. Providers can confirm suspected illegal robocall traffic by using “content analytics.”¹⁰⁵ As a way to control the torrent of unwanted calls, YouMail, and other service providers to the telephone industry, have been given access by their customers to their voicemail. Other service providers have their own “honey-pots” (telephone numbers owned by the recipient to monitor patterns of illegal calls) to capture information about illegal calls. Recordings of the scam calls are captured on these millions of voice mailboxes, which then enable the providers to determine the true intent of these calls through the words used in the message left on the voicemail.¹⁰⁶ Using this “content analytics” method, these providers are then able to block the transmittal of similar calls deemed to be illegal.¹⁰⁷

One provider blocking illegal calls will not resolve the problem, as scam callers will simply find another call path to reach vulnerable Americans' phones (and their pockets). Unless all U.S. providers implement appropriate blocking protocols, scammers will still be able to find a way to defraud American phone subscribers.

Because voice service providers make money from connecting calls, whether those calls are legitimate or not, voice service providers are incentivized to look the other way and accept payment for permitting illegal traffic to reach American phones. That incentive structure needs to change. In September 2021, FCC Commissioner Geoffrey Starks noted this counterproductive dynamic regarding robocalls: “[I]llegal robocalls will continue so long as those initiating and facilitating them can get away with and profit from it. Last year’s estimated 46 billion robocalls and last month’s estimated 4.1 billion calls are proof positive of that.”¹⁰⁸

As described in Section IV, the FCC has not yet taken effective action to stop these scam robocalls. Unfortunately, the providers complicit with the scam robocallers will continue to dump scam traffic into the American phone system so long as it is profitable for them to do so.

E. Providers have a system to filter out some spam texts, but it is insufficient.

As explained in Section II, the number of scam texts is also increasing. This is so despite the voluntary registry established by the major cell phone providers. Senders who join the registry must abide by registry rules, such as allowing the registry to categorize the type of sender and the content of the messages, and requiring registry texts to contain a “stop” mechanism, which informs recipients that they can request that texts from that text sender no longer be sent.¹⁰⁹ In return for using the registry for text campaigns,¹¹⁰ text senders are charged less for registry-compliant messages than text campaigns that are not sent through the registry.¹¹¹ By offering discounted prices for texts sent in compliance with their rules,¹¹² the registry gives an incentive to text senders to use the registry. The registry blocks texts sent through the registry that are patently fraudulent.

However, the use of the registry is voluntary, and its rules apply only to texts sent through the registry. There is no rule or mechanism that requires participation in the registry or prevents automated text messages from being sent without being submitted to the registry. Text scammers have no reason to follow these registry rules.

IV. THE U.S. GOVERNMENT HAS NOT BEEN ABLE TO STOP THE SCAM CALLS.

The goal of the Telephone Consumer Protection Act, passed by Congress in 1991, was to give telephone users some control over automated calls.¹¹³ Yet, as virtually every telephone subscriber in 2022 knows, the problem of unwanted calls has continued to escalate.

In a further effort to address illegal robocalls as well as the mushrooming problem of callers using fake caller IDs (referred to as spoofing), Congress passed the TRACED Act in 2019.¹¹⁴ Since then, the FCC has adopted several regulations and is proposing additional initiatives to combat fraudulent calls. However, despite these efforts, in each of the past two years more than **20 billion scam robocalls** were made to U.S. telephone subscribers.¹¹⁵

A. The Federal Communications Commission's (FCC's) approach to regulating robocalls has not solved the problem.

This is in no small part due to the Commission's approach to regulating robocalls—for more than two years, the Commission has made it clear that it expects providers to couple STIR/SHAKEN (or other “reasonable measures” of call authentication) with reasonable use of call analytics, and that providers are permitted (but not required) to block calls likely to be illegal.¹¹⁶ In so doing, the Commission has placed the emphasis on reasonableness and provider discretion, rather than on effectiveness at actually stopping robocalls.

Unfortunately, while the FCC has initiated numerous proceedings to deal with illegal robocalls, we believe that none of these, either singly or in combination, will effectively stop most of the illegal calls, for these reasons:

- Requiring STIR/SHAKEN attestation only requires telecommunications providers to assess the reliability of the caller IDs attached to calls. Even full compliance will not stop the scam callers.
- No existing or proposed rule or policy requires all providers to act affirmatively to stop criminal robocalls; providers are permitted to wait for the FCC to tell them to take action.
- Existing and proposed regulations designed to prevent illegal robocalls generally consider providers to be compliant if they have a policy or procedure in place, rather than measuring compliance based on results.
- There is no automatic mechanism for suspending noncompliant providers from the network, and no limitation preventing individuals who have processed criminal robocalls in the past from simply creating a new company under a different name and continuing to transmit illegal calls.

- The powerful Traceback tool is not being utilized effectively.

As this report went to print, the FCC announced a vote on new regulations and proposed regulations for Gateway Providers.¹¹⁷ Our preliminary evaluation suggests that this order largely represents more of the same approach from the FCC. As such, all of our concerns will likely remain, however that will depend on what the FCC ultimately issues in its final orders.

1. The FCC permits but does not require providers to block illegal calls. In 2017, the FCC clarified that voice service providers were permitted to block calls considered “highly likely to be illegal” because they appeared to be from numbers that were not in use.¹¹⁸ This permission was extended in 2020 to allow providers to use “reasonable analytics to provide network-based blocking” of calls “highly likely to be illegal.”¹¹⁹ Neither of these measures *requires* providers to block these calls. Since providers are paid per answered call that they transmit,¹²⁰ it should not be a surprise that giving them permission to block calls has not been effective these past five years. The enormous numbers of fraudulent calls that continue to reach American consumers shows that providers need to be required to identify and block illegal calls.

2. Addressing caller-ID spoofing will not stop scam robocalls. The TRACED Act required the FCC to implement the STIR/SHAKEN methodology to authenticate caller IDs associated with robocalls.¹²¹ Implementation has been mandated for most of the industry and will certainly help reduce telemarketers’ use of spoofed caller IDs. However, applying the STIR/SHAKEN methodology is unlikely to cause a significant decrease in scam robocalls.

STIR/SHAKEN requires only that originating providers apply a certification to each call that indicates how confident the provider is that the caller ID accompanying the call is correct.¹²² An originating provider is considered to be in full compliance with STIR/SHAKEN even when it merely gives calls a B level attestation (indicating that the provider is not sure), or a C level attestation (indicating that it has no ability to authenticate the source of the call).¹²³ Those attestations do little to ensure that the caller IDs accompanying the calls are truthful.¹²⁴

More fundamentally, complying with STIR/SHAKEN only establishes that the caller ID is not spoofed. As long as telecommunications providers are allowed to rent rotating series of numbers to their customers making illegal calls, the caller ID may be truthful, since the caller has the right to use the rented numbers when the calls are made, but the ID information itself will be meaningless. As the telephone number identified is only fleetingly associated with the caller, it does not provide an effective way to identify the caller or even block the caller’s calls.

3. The Robocall Mitigation Database does not stop scam robocalls. As of June 30, 2021, originating voice service providers must certify in the newly created Robocall Mitigation Database (RMD) that they have implemented STIR/SHAKEN for that part of their networks that use internet protocols.¹²⁵ Providers that do not use the internet to transmit calls must have alternative robocall mitigation plans.¹²⁶ And some small providers have been granted an extension until June 30, 2022 to comply with STIR/SHAKEN,¹²⁷ as long as they certify in the RMD that they are employing an alternative robocall mitigation program. Effective September 28, 2021, the FCC prohibits intermediate and terminating providers from accepting telephone traffic directly from any providers not listed in the RMD.¹²⁸

An access barrier like the RMD could be a powerful tool to stop scam calls. However, for reasons described in #2, *supra*, its focus on compliance with STIR/SHAKEN means that the RMD will not stop scam calls. Moreover, there is no requirement, much less an automated mechanism, that non-compliant providers be suspended from the RMD,¹²⁹ and the FCC does not have the scale to monitor compliance by each of the 4,000 providers that have registered.

In addition, because there are such low entry requirements for setting up business as a VoIP provider, there is no meaningful barrier to stop providers who have been caught from simply setting up shop using a different name and continuing with the same illegal behavior.¹³⁰ Any provider anywhere in the world can create an entry in the RMD by filling in a form and clicking a few boxes. As a result, in its current configuration the RMD is of limited use in ensuring compliance even with the STIR/SHAKEN protocol, let alone with engaging in effective robocall mitigation.

4. The powerful potential of ITG Tracebacks is underutilized. Pursuant to the direction in the TRACED Act the FCC selected USTelecom (a trade association for telephone companies and providers of broadband service) to conduct tracebacks of suspected unlawful robocalls.¹³¹ As described in Section III D, *supra*, the ITG traces suspicious traffic from the terminating provider back through intermediate providers to the gateway or originating provider and then to the caller, when the originating provider provides that information in the traceback.¹³² Each provider in the call path is notified that the call being traced was illegal and each provider is generally given the content of the illegal call. However, although the ITG *may* refer the information from tracebacks to state or federal enforcement authorities, there is no requirement that it does so.¹³³

The ITG conducted more than 5,400 tracebacks in 2020 and 2021.¹³⁴ However, the details about these tracebacks are not disclosed. If revealed, this traceback work could have a profound effect on stopping illegal calls, but its potential is not being used. First, information about completed tracebacks would have enormous

value to providers seeking to avoid transmitting scam calls, as it would enable them to identify and avoid accepting calls from the gateway, originating, and intermediate providers that have been found in previous tracebacks to have repeatedly transmitted these calls. Making traceback requests public would also enable attorneys general and scam victims to identify complicit providers and hold them liable. All these steps would place market pressure on originators and facilitators of scam calls. Yet nearly all the information regarding tracebacks is currently secret, available only to the ITG itself and provided to the FCC, the FTC or state AGs based on non-public rules.

The FCC does include information about tracebacks in its annual report to Congress. This report is of little use to providers and others in identifying entities to which fraudulent calls have been repeatedly traced, however, because it does not distinguish problematic providers from cooperative providers. The Commission reports providers as either participating in traceback; being non-responsive to one or more tracebacks; or being non-responsive to three or more consecutive tracebacks. But merely responding to traceback requests does not show providers are complicit in transmitting illegal calls, as traceback requests typically start with the terminating provider that transmitted the call to the called party, which usually occurs after the illegal calls have been so mixed in with legitimate calls that they cannot be identified. As a result, the Commission's 2020 and 2021 reports to Congress present providers such as thinQ,¹³⁵ RSCoM,¹³⁶ Piratel,¹³⁷ and Globex¹³⁸ that have been defendants or respondents in enforcement actions as being just as cooperative as the likes of Verizon and AT&T.¹³⁹

Second, there is insufficient follow-up on tracebacks by enforcement authorities. Once the ITG has completed a traceback of a suspected illegal call, it is allowed to but not required to refer the information to state or federal enforcement authorities.¹⁴⁰ Even though ITG conducted more than 5,400 tracebacks in 2020 and 2021¹⁴¹—many against the same providers—the FCC sent only 18 cease and desist letters between January 1, 2021 and April 1, 2022.¹⁴² The FCC has not sent any cease and desist letters against Articul8, the defendant in the case brought by the North Carolina Attorney General, even though Articul8 had 49 tracebacks.¹⁴³ The FCC sent a cease and desist letter to TCA VoIP, the defendant in the Vermont Attorney General's case, only a few weeks before that case was filed, even though TCA VoIP had been the recipient of 132 tracebacks over a period of two years.¹⁴⁴ In addition, while the TCPA regulations were amended in 2021 to require voice service providers to respond to tracebacks,¹⁴⁵ there is no provision for automatically suspending those who do not comply from the Robocall Mitigation Database.

5. The requirement that originating providers “Know Your Customer” does not stop the illegal calls. Both Congress and the FCC have recognized that the “rising tide of robocalls and the emergence of VoIP go hand in hand.”¹⁴⁶ Section 6 of the TRACED Act required the FCC to initiate proceedings to require VoIP providers to “know their customers.”¹⁴⁷

In 2021, the FCC amended its regulations to add a requirement that each voice service provider “[t]ake affirmative, effective measures to prevent new and renewing customers from using its network to originate illegal calls, including knowing its customers and exercising due diligence in ensuring that its services are not used to originate illegal traffic.”¹⁴⁸ However, in its May 2022 order, the FCC may impose additional requirements for providers to describe how they will “know” their upstream providers (see # 6 *infra*).

This requirement is a good start, but it has significant loopholes. First, it appears to apply only to providers whose customers “originate” calls, so is not clearly applicable to gateway providers that transmit calls from abroad, or to intermediate providers that accept calls from either originating, gateway or other intermediate providers. Second, it does not include a clear rule requiring that downstream intermediate providers or terminating providers that are capable of identifying suspicious traffic block illegal calls from reaching their customers. In addition, the FCC has not brought any action to date for violating these requirements, nor has it articulated a clear enforcement mechanism.

6. The pending proceedings for problematic VoIP providers and gateway providers would only require certifications and policies. As of April 2022, the FCC has initiated two additional proceedings to address illegal robocalls. In the first, recognizing that the illegal problem calls are typically made through small VoIP providers, the FCC has proposed that VoIP providers be required to certify “that the provider will not assist and facilitate illegal robocalling, illegal spoofing, or fraud, and that it will take reasonable steps to cease origination, termination, and/or transmission of illegal robocall traffic once discovered.”¹⁴⁹ The proposal also would require VoIP providers to “certify that its traffic is signed with STIR/SHAKEN or is subject to a robocall mitigation program in order to file in the Robocall Mitigation Database.”¹⁵⁰ However, this proposal does not include any mechanism for suspending a provider from the RMD that has been determined to have a) transmitted illegal calls, b) certified its traffic incorrectly, or even c) failed to respond to traceback requests. Additionally, it requires “reasonable steps” rather than “effective measures,” meaning that providers are off the hook if they have procedures designed to address robocalls, regardless of whether their efforts are actually effective in reducing robocalls.

In the second proceeding relating to gateway providers, the FCC requested comments on how to prevent foreign-originated illegal robocalls from entering

the American telephone network through gateway providers.¹⁵¹ The Commission proposed a myriad of potential steps that gateway providers could be required to take to limit the flood of illegal calls from abroad. But, even if the steps all are ordered, the regulatory structure would still seem to allow providers to evade the consequences of transmitting illegal calls so long as the providers had “policies and procedures” designed to avoid transmission of calls, instead of simply requiring that providers ensure that they do not transmit illegal calls. Additionally, providers downstream from the gateway providers would be permitted to delay blocking bad-actor gateway providers until receiving notification from the Commission.¹⁵²

7. Proposed Limitation of Access to Numbers by VoIPs. Currently, VoIP providers are permitted access to large numbers of telephone numbers which they can rent to their caller-customers to use on a rotating basis.¹⁵³ Callers can then rotate through these rented numbers to make only a few calls using each number. This allows these illegal calls to evade the analytics applied by downstream providers attempting to identify—and then block—illegal robocalls. (Some complicit VoIP providers even advertise access to this system to attract illegal callers.¹⁵⁴) As there is no good reason for this proliferation of numbers, the FCC is considering how VoIP providers should be limited to direct access to telephone numbers, as required by Section 6 of the TRACED Act.¹⁵⁵

Unfortunately, the FCC only proposes to require the VoIP providers to certify that they will use numbering resources lawfully, and to describe in the RMD their steps to ensure compliance.¹⁵⁶ Requiring the very VoIPs that have been deliberately facilitating illegal calls to American subscribers to adopt procedures and make a promise that they will operate “lawfully” seems like an exercise in futility. It would be much more effective to require all originating and intermediate VoIPs to monitor their traffic, and then to require that access to the network be terminated for any providers found to be transmitting illegal calls.¹⁵⁷

8. The FCC’s enforcement actions have not been sufficient to stop or slow the scam calls. The FCC’s enforcement efforts consist largely of sending cease and desist letters to providers that have been determined through the traceback process to have repeatedly made illegal calls, and six enforcement actions.¹⁵⁸ But of the more than 5,400 tracebacks ITG conducted in 2020 and 2021¹⁵⁹—many against the same providers—as of the time of this writing, the FCC has announced only 18 cease and desist letters since January 2021.¹⁶⁰

Another weakness is that, even when a particular provider has been the respondent in an enforcement effort brought by the FCC—such as John Spiller was in 2020¹⁶¹—there is currently nothing to stop that provider from recasting itself under a different name and resuming its illegal business practices. Indeed, this seems to be exactly what was done by John Spiller, who faced the FCC’s

largest fine of \$225 million, did not pay it, and apparently continued in the same business.¹⁶² The ease of re-registering in the RMD creates the concern that fraudulent callers will still be able to use this revolving door tactic.

Moreover, these enforcement methods are all reactive rather than proactive. They are brought only *after* the billions of calls were made, the privacy of tens of millions of subscribers has been violated, and millions of consumers have lost money to the scams perpetrated in the robocalls. Instead of relying on after-the-fact cease-and-desist orders and forfeitures, little of which is ever collected, the FCC should require all providers in the call path to proactively employ analytics and other tools to identify illegal calls, and then refuse to transmit them. This more proactive approach would protect not only consumers, but would also benefit legal robocallers, whose calls will be less likely to be improperly labeled or blocked.

B. The Federal Trade Commission's (FTC's) enforcement of the Telemarketing Sales Rule (TSR) is unlikely to stop the illegal calls.

The Telemarketing Sales Rule prohibiting deceptive and abusive telemarketing acts and practices,¹⁶³ issued by the Federal Trade Commission, declares it a deceptive act for a person to provide substantial assistance to a telemarketer while knowing, or consciously avoiding knowledge, that the telemarketer is violating the TSR.¹⁶⁴ An individual or company that provides substantial assistance can be held liable for a TSR violation even without meeting the definition of “seller” or “telemarketer,”¹⁶⁵ so a VoIP provider that knows or consciously avoids knowing that the calls it transmits are fraudulent can be held liable under this standard.

The FTC has been using its authority under the TSR to investigate and punish VoIP providers that have transmitted millions of illegal robocalls. It has issued several civil investigative demands against VoIP providers,¹⁶⁶ and successfully sued other VoIP providers, resulting in substantial fines and lifetime bans from engaging in the business.¹⁶⁷ The FTC also issued 19 warning letters in early 2020 to VoIP providers.¹⁶⁸ Unfortunately, the FTC's actions to date have not created sufficient incentives among VoIP providers to stop the transmittal of illegal robocalls. As this report went to print, the FTC voted on new proposed regulations for telemarketers, including record-keeping requirements, and extending the protection of the TSR in the realm of business to business (B2B) telemarketing and inbound calling.¹⁶⁹ While these measures will bolster enforcement of the TSR, they are unlikely to stop the calls from coming in the first place because not all providers are adequately incentivized to stop accepting illegal traffic.

V. THE FCC CAN STOP MOST SCAM ROBOCALLS AND ILLEGAL TEXTS—HERE IS HOW.

Every month in which the issue of scam robocalls is not meaningfully resolved, more than one billion more scam calls assault American subscribers, and millions lose money to those scams. The current system protects providers, rather than ensuring the protection of the American subscribers from fraudulent robocalls.

These scam robocalls are transmitted as the result of the choices made by service providers regarding what calls they accept payment for transmitting. The originating provider makes a choice to accept calls from a certain robocaller and sends those calls to an intermediate provider who chooses to accept and transmit those calls down the call path. If that first intermediate provider decides not to accept the calls from the originating provider, the scam calls are stopped at that point and do not reach the called party unless the originating provider finds another intermediate provider willing to take them. Similarly, each hop in the chain to a subsequent intermediate provider or the terminating provider represents a separate decision by the downstream provider to accept and transmit those calls or to block them. Currently, the primary determinant for many of these instantaneous decisions made by the providers in the call path is profit. That must change.

We propose that, to stop the criminal robocalls, three principles must be paramount:

1. All providers in the call path should have an affirmative obligation to engage in effective mitigation against illegal robocalls.
2. Providers who knew or should have known that they were transmitting illegal robocalls should face clear financial consequences.¹⁷⁰
3. Law enforcement, telephone service providers, victims of scam calls, legal robocallers, and the general public should have access to all available information about the sources of the illegal robocalls and their complicit providers.

Much of what we say in the five proposals below is supported by various arms of the telecom industry, and state regulators.¹⁷¹

Proposal 1: Require that all providers in the call path engage in effective mitigation against illegal robocalls.

Current FCC rules only *permit* intermediate providers to stop scam calls, rather than require them to do so.¹⁷² Likewise, terminating providers are permitted, rather than required, to block calls when analytics indicate that the calls are likely illegal.¹⁷³ Providers are only required to “effectively mitigate illegal traffic when

[they] receive actual written notice of such traffic from the Commission. . . .”¹⁷⁴ Originating providers—and now—gateway providers are required to take “effective measures” to prevent their customers from using their networks to transmit illegal calls. However, gateway providers are still not required to block illegal calls (except those on a “Do Not Originate” list) until notified by the Commission to do so.”¹⁷⁵

The FCC regulations should be changed to require that all providers, including intermediate providers, use all available methodologies and block scam calls as soon as they are discovered.

Intermediate providers, especially those in upstream positions that accept calls directly from originating or gateway providers, are often in the best position to recognize and block illegal calls. They should be required to do so.

Terminating providers may be less able to block individual calls on the basis of behavioral analytics because they receive so many calls from intermediate providers who are far down the call path from the initial intermediate providers (those accepting calls from the originating providers). But terminating providers have the power to require that their directly upstream intermediate providers not accept illegal calls from their respective (further) upstream providers. The upstream providers, using either traceback information or content or behavioral analytics, can more easily block fraudulent calls.

The terminating providers can protect themselves, for example, by requiring that the upstream providers sending them calls impose the same mandate on their upstream providers. In this way, the marketplace can impose the same conditions all the way upstream to the originating or gateway providers. The FCC should structure the blocking requirements so that providers are either required to, or have strong incentives to, refuse to accept future calls from upstream providers that have transmitted scam calls, as indicated by tracebacks or call or traffic analytics.

Proposal 2: Clear financial consequences should apply to providers who transmit illegal robocalls when they knew or should have known that the calls were illegal.

As described in Section III there are tools currently available that allow providers to identify and then block scam robocalls. But providers need to be incentivized to use these tools and to block the calls found to be illegal. As described by one FCC Commissioner, “illegal robocalls will continue so long as those initiating and facilitating them can get away with and profit from it.”¹⁷⁶

The choices that providers in the call path make about whether to accept calls from upstream providers should be guided not only by the price paid for those calls, but also by the risk involved in accepting calls from those upstream providers. The consequences of the wrong choice should be steep.

The Fair Credit Billing Act (FCBA),¹⁷⁷ which governs the relationship between banks and consumers who use credit cards, illustrates why placing the financial liability on providers for illegal calls will be an effective mechanism to stop scam robocalls. The FCBA imposes the cost of losses from credit card fraud and error on the banks, rather than consumers. As a result, the banking industry has developed a robust set of protections governing the use of credit cards to minimize their own losses from theft, fraud and even user negligence. The banks control the system, imposing on merchants their requirements to protect against losses. While there are extensive regulations issued by federal regulators that govern the transactions between the banks and their customers (e.g., disclosures and rules governing imposition of finance charges), there are no rules governing *how* the banks should protect themselves from losses caused by fraudsters. The banks—which will bear the burden of failure—have every incentive to develop vigorous procedures to limit these losses. The security procedures used by banks to monitor and avoid losses is constantly changing, to combat new threats.

The telephone service providers should be similarly incentivized to develop and use procedures to guard against transmitting fraud robocalls.

The rules should clearly state that all providers in the call path of a fraudulent call are liable for the consequences of that call if the provider knew or should have known that the call was illegal. Pursuant to Proposal 1, this would apply to nearly all illegal calls, as all providers in the call path would be required to use every available mitigation tool to determine the illegality of the calls, and then block them.

We do not recommend that the FCC prescribe the specific methods of implementation necessary to stop the transmission of illegal robocalls effectively. Just as the FCBA does not tell banking institutions how to prevent frauds and other losses, the FCC's rules should simply provide the incentive for the telephone service providers to find and use every available, reasonable method of detecting and blocking the illegal calls. But to illustrate how this might work, we offer suggestions and examples of how providers might achieve this.

For originating, gateway, and first intermediate providers specifically, there is little excuse for continuing to transmit scam robocall traffic after any notice that the traffic is illegal based on previous tracebacks or FCC cease and desist letters. But these providers also must be incentivized to employ additional tools, such as behavioral analytics (e.g. the patterns of the calls sent from that provider, such as the duration of the calls, and the number of different caller IDs used, etc.), and to analyze the content of the calls (capturing and reviewing the messages in the robocalls).¹⁷⁸ Additionally, contracts between providers should require that calls from upstream providers will stop being accepted if, for example, the upstream provider has a history of transmitting illegal calls, fails to respond to tracebacks,

or other analytics indicate that calls from the provider are likely illegal. Providers who do not include and enforce such terms in their contracts should be held liable for the fraud losses suffered by consumers.¹⁷⁹

Requiring bonds for providers (see Proposal 5, *infra*) can also address concerns regarding providers who might not have sufficient financial capital to compensate consumers for their losses.

Proposal 3: The FCC should use suspension¹⁸⁰ from the Robocall Mitigation Database as a mechanism to protect telephone subscribers from receiving illegal calls, pending investigations. This would place a higher priority on protecting U.S. telephone subscribers from criminal scam calls and texts, than on providing VoIP originating and gateway providers access to the U.S. telephone network. To accomplish this, we recommend the following possible triggers for suspension:

- a. The provider knows, or consciously avoids knowing, that it has transmitted illegal calls into the U.S. telephone network, subject to appropriate safe harbors established by the FCC;
- b. The ITG has conducted a subsequent traceback that identifies a VoIP provider that had previously either (i) originated criminally fraudulent calls to American telephone numbers or provided gateway services to callers making such calls, or (ii) been the first intermediate provider of services to the originating or gateway provider described in subsection (i);
- c. The provider fails to respond to a traceback request with 48 business hours from a request from the ITG;¹⁸¹ or
- d. The provider is determined to be owned or operated by any individuals who owned or operated VoIP providers previously punished or sanctioned by the FCC, or any other federal or state law enforcement agency, for providing service to callers making illegal calls.

Safe harbors might be permitted for terminating and downstream providers who are unable to block individual scam robocalls because of the way in which the calls are delivered to them, so long as these providers are otherwise engaged in effective mitigation.¹⁸²

Proposal 4: All tracebacks conducted by the ITG should be made public. Making tracebacks public will enable providers throughout the call path to identify the sources of illegal calls and use their market power to prevent those calls from reaching subscribers.¹⁸³

Legal robocallers will also benefit if tracebacks are made public. They will be able to require that their originating providers not transmit calls through any intermediate providers that have been repeated recipients of tracebacks.

These legal robocallers will be empowered to protect their calls from being inappropriately blocked or misidentified because their calls were transmitted through providers that had a history of transmitting illegal calls.

To accomplish this, the FCC should require that all tracebacks conducted by the ITG be made public within 24 hours of the traceback. To ensure the privacy of the subscribers receiving the calls, the last four digits of the subscriber's telephone number in each traceback should be redacted.

Proposal 5: The FCC should impose (or be empowered to impose) strict licensing and high bonding requirements for VoIP providers, subject to an exception for providers with a strong history of compliance. To accomplish this, the FCC should require that VoIP providers:

- a. Submit to the Commission an application for a license, or a renewal of an existing license, that includes the names and contact information of the individuals who own the provider or, if the provider is a corporation, the majority shareholders of the corporation and other parties of interest with respect to the management of the provider, as determined appropriate by the Commission to ensure that persons with a history of transmitting calls in violation of this section are ineligible for such a license;
- b. Provide to the Commission evidence that the provider has posted a surety bond of \$1,000,000, or such additional amount that the Commission may require based on the provider's record of transmitting illegal calls.

The scourge of scam robocalls and texts is responsible for more than one billion illegal calls every month—while merely annoying to some, to many vulnerable Americans these scam messages are ruinous. Although the FTC, the FCC, and some telecom companies have undertaken extensive efforts to remedy the problem, we are not optimistic that they will achieve their purported goal unless: providers are required to employ effective mitigation strategies (not merely “reasonable steps”), and providers are financially punished when those strategies fail to protect consumers from scam messages. Finally, to maximize swift and effective measures to protect consumers, information about tracebacks and other determinations that providers are transmitting illegal robocalls should be made public.

ENDNOTES

1. See 47 U.S.C. § 227(a). [Federal Trade Comm'n, Consumer Advice, Robocalls](#) (“If you answer the phone and hear a recorded message instead of a live person, it’s a robocall.”).
2. 47 U.S.C. § 227. The TCPA also makes it illegal to use an automated telephone dialing system (ATDS or autodialer) to call a phone subscriber without first obtaining consent, with a few exceptions.
3. 47 U.S.C. § 227(b)(1).
4. Americans are losing significant amounts to *live* scam calls as well. However, those live calls are beyond the scope of this report. See, e.g., Public Service Announcement, Federal Bureau of Investigation, [FBI Warns of the Impersonation of Law Enforcement and Government Officials](#) (Mar. 7, 2022).
5. According to estimates from YouMail, since 2018, no fewer than 45.87 billion robocalls have been sent to American phones in a calendar year, with no fewer than 37% and as many as 46% of these calls representing scam robocalls. Dividing this minimum annual number by 12 to approximate a monthly average, and assuming the minimum estimated percentage of 37%, our conservative estimate is that more than 1.4 billion scam robocalls are made to American phones every month. YouMail estimates that there were 47,839,232,200 placed in 2018, 58,536,224,700 placed in 2019, 45,866,949,500 placed in 2020, and 50,507,702,500 placed in 2021. YouMail, [Historical Robocalls By Time](#). YouMail estimates that 37% of robocalls placed in 2018 were scam robocalls. PR Newswire, [Nearly 48 Billion Robocalls Made in 2018, According to YouMail Robocall Index](#) (Jan. 23, 2019). YouMail estimates that 44% of robocalls placed in 2019 were scam robocalls. PR Newswire, [Americans Hit by Over 58 Billion Robocalls in 2019, Says YouMail Robocall Index](#) (Jan. 15, 2020). YouMail estimates that 46% of robocalls in 2020 were scam robocalls. PR Newswire, [Americans Hit by Just Under 46 Billion Robocalls in 2020, Says YouMail Robocall Index](#) (Jan. 26, 2021). YouMail estimates that 42% of robocalls in 2021 were scam robocalls. PR Newswire, [U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#) (Jan. 6, 2022).
6. See *id.*
7. YouMail confidential data provided to NCLC [hereinafter YouMail Data Provided to NCLC]. After identifying the top 1,000 scam campaigns in a single month and examining the calls made in January 2022 by only those top campaigns, YouMail indicated in its private data that more than 458 million scam robocalls were made by the top 1,000 scam robocall campaigns in that 30-day period.
8. Frank Green, [Chesterfield woman's life is upended in \\$10 million robocall scam](#), Richmond Times-Dispatch, June 10, 2021. [Another example of this type of call is available here.](#)
9. There were over 8.6 million of these types of calls made in January 2022. YouMail Data Provided to NCLC, *supra* note 7.
10. This number is reached by combining fraud reported by age 60-69, 70-79, and 80+ (521MM+364MM+149MM = 1.034BB). See FTC Consumer Sentinel Network, [Reported Frauds and Losses by Age, Year: 2021](#) (updated Feb. 22, 2022) (Age & Fraud tab, Year 2021, with quarters 1 through 4 checked).
11. Stephen Nessen, NPR, [Chinese Robocalls Bombarding the US Are Part of an International Phone Scam](#) (May 10, 2018).
12. YouMail estimates that in January 2022 there were over 12.3 million disability benefits scam robocalls. YouMail Data Provided to NCLC, *supra* note 7. [A typical recording is available here.](#)

13. YouMail estimates that in January 2022 there were over 32.6 million student loan scam robocalls. YouMail Data Provided to NCLC, *supra* note 7. [A typical recording is available here.](#)
14. YouMail estimates that over **114 million of these scam robocalls** caused U.S. telephones to ring in January 2022. YouMail Data Provided to NCLC, *supra* note 7. [A recording of a sample call is available here.](#)
15. YouMail estimates that over **25.6 million of these Medicare scam robocalls** rang on subscribers' phones in January 2022. YouMail Data Provided to NCLC, *supra* note 7. [A recording of a sample call is available here.](#)
16. YouMail estimates that over 70 million health insurance scam robocalls rang on subscribers' phones in January 2022. YouMail Data Provided to NCLC, *supra* note 7. [A recording of just one of many health insurance campaign scam calls is available here.](#)
17. YouMail estimates that over 15.8 million bill reduction scam robocalls rang on subscribers' phones in January 2022. YouMail Data Provided to NCLC, *supra* note 7. [A recording of just one of many fake bill reduction campaign calls is available here.](#)
18. YouMail estimates that over 140,000 IRS scam robocalls rang on subscribers' phones in January 2022. YouMail Data Provided to NCLC, *supra* note 7. See Courier Video, [Fake IRS Scam Recording](#), YouTube (Jul. 2, 2017) (last visited Feb. 10, 2022).
19. YouMail estimates that over 19.5 million business impersonation scam robocalls rang on subscribers' phones in January 2022, with more than 13.7 million scam robocalls relating explicitly to Amazon (including fake fraud alert and automatic charge scams). YouMail Data Provided to NCLC, *supra* note 7. [A recording of a sample call is available here.](#) See also Hiya, [State of the Call 2022 Report 7](#) (2022) (noting that 62% of phone subscribers surveyed reported having received a business impersonation scam call in 2021). The FTC reported consumer financial losses from business impersonation scams (by any contact method, not just phone) more than tripled between 2019 and 2021, exceeding \$451 million in 2021 alone. Press Release, Federal Trade Comm'n, [FTC Outlines Aggressive Approach to Policing Against Pandemic Predators in Testimony Before Senate Commerce Subcommittee](#) (Feb. 1, 2022). Regarding Amazon impersonations specifically, the FTC reported that more than one in three complaints (36%) about business impersonation scams in the twelve-month period preceding July 2021 were from scammers claiming to be Amazon. Emma Fletcher, Federal Trade Comm'n Data Spotlight, [Amazon tops list of impersonated businesses](#) (Oct. 20, 2021) (6% of scammers claimed to be Apple).
20. The robocall blocking company YouMail has thousands of recordings of such fraud campaigns.
21. See Federal Commc'ns Comm'n, [Caller ID Spoofing](#).
22. This is called "neighbor spoofing." See Better Business Bureau, [BBB Scam Alert: "Neighbor spoofing" is a common type of phone scam](#) (May 29, 2020).
23. See YouMail, [What Everyone Needs to Know about Leased Telephone Numbers and Unwanted Robocalls](#), presentation at SIPNOC 2022 Webinar Series (Mar. 21, 2022) [hereinafter *What Everyone Needs to Know*]. See also [In re Call Authentication Trust Anchor, Second Report and Order](#), WC Docket No. 17-97, at ¶ 50 (Rel. Oct. 1, 2020), [hereinafter *Oct. 1, 2020 Second Report and Order*] (noting that some providers lease numbers and do not have direct access to numbering resources).
24. See FTC Consumer Sentinel Network, [Fraud Reports by Contact Method, Reports and Amounts by Contact Method](#) (updated Feb. 22, 2022) (Losses & Contact Method tab, with quarters 1 through 4 checked for 2021 and 2020; indicating 644,048 fraud reports using the phone call contact method and 377,840 using the text contact method from Q1-Q4 2021, as compared with 382,036 phone call and 334,952 text fraud reports for Q1-Q4 2020).

25. The 60% figure is consistent with Truecaller data. Truecaller, [Truecaller Insights 2021 U.S. Spam and Scam Report](#) (June 28, 2021) [hereinafter Truecaller Insights]. By quoting Truecaller's statistics, we are not endorsing Truecaller's business model, as we are aware of concerns that have been raised. See, e.g., Alfred Ng, CNET, [Those robocall blocker apps are hanging up on your privacy](#) (Aug. 10, 2019); Rest of World, [How Truecaller built a billion-dollar caller ID data empire in India](#) (Mar. 2022).
26. In calculating this figure, we assumed that 100% of scam texts were automated, but, consistent with Truecaller's estimate, that only 60% of the scam calls were robocalls.
27. FTC Consumer Sentinel Network, [Fraud Reports by Contact Method, Reports & Amount Lost by Contact Method](#) (updated Feb. 22, 2022) (Losses & Contact Method tab, with quarters 1 through 4 checked for years 2017 through 2021).
28. Truecaller Insights, *supra* note 25 (reporting on results of Harris Poll surveys). Truecaller's data includes scam calls reported as robocalls, as well as calls that were not identified as robocalls, although many calls that appear to be live calls are likely calls made with prerecorded voices and artificial intelligence, which are in fact robocalls. See Appendix 1, *infra*.
29. Truecaller Insights, *supra* note 25.
30. This figure represents an increase of greater than 50% from \$19.7 billion in 2020. Truecaller Insights, *supra* note 25.
31. FTC Consumer Sentinel Network, [Fraud Reports by Contact Method, Reports and Amounts Lost by Contact Method, Year: 2021](#) (updated Feb. 22, 2022). Note that this figure captures consumer complaints for all scam calls, not just those scam calls reported as robocalls, and that it likely understates the magnitude of the problem, as only a small percentage of consumers go through the trouble of filing a complaint.
32. FTC Consumer Sentinel Network, [Fraud Reports by Contact Method, Reports and Amounts Lost by Contact Method, Year: 2021](#) (updated Feb. 22, 2022)
33. FTC Consumer Sentinel Network, [Percentage Reporting a Fraud Loss and Median Loss by Age, Year: 2020](#) (updated Feb. 22, 2022) (Age & Fraud Losses tab with 2020 (the most recent year available) checked).
34. FTC, [Protecting Older Consumers 2020-2021](#), 34-35 (Oct. 18, 2021). This report also observed that the median loss for consumers aged 60+ was significantly higher for telephone-based frauds than other contact methods in 2020: \$1,800 for phone as compared with approximately \$1,000 for text or mail, and \$500 or less for other methods. *Id.* at 36.
35. Truecaller Insights, *supra* note 25. To underscore how severely fraud is underreported, compare Truecaller's estimates of \$10.5 billion, \$19.7 billion, and \$29.8 billion for 2019, 2020, and 2021, respectively, with the FTC's reported complaint totals of \$400,000 to \$700,000 per year for all scam calls over that same time frame. *N.B.* In both instances, these estimates include some live scam calls.
36. See *In re* Advanced Methods to Target and Eliminate Unlawful Robocalls and Call Authentication Trust Anchor, [Declaratory Ruling and Third Further Notice of Proposed Rulemaking](#), CG Docket No. 17-59 and WC Docket No. 17-97, FCC 19-51, at ¶ 40 (Rel. June 7, 2019); *In re* Call Authentication Trust Anchor and Implementation of TRACED Act Section 6(a)—[Knowledge of Customers by Entities with Access to Numbering Resources, Report and Order and Further Notice of Proposed Rulemaking](#), WC Docket Nos. 17-97, 20-67, FCC 20-42, at ¶ 47 (Rel. Mar. 31, 2020); Press Release, Federal Commc'ns Comm'n, [FCC Mandates That Phone Companies Implement Caller ID Authentication to Combat Spoofed Robocalls](#) (Mar. 31, 2020) ("The FCC estimates that the benefits of eliminating the wasted time and nuisance caused by illegal scam robocalls will exceed \$3 billion annually, and STIR/SHAKEN is an important part of realizing those cost savings.").

37. See Octavio Blanco, Consumer Reports, [Mad About Robocalls?](#) (Apr. 2, 2019).
38. See Tim Harper, Consumer Reports, [Why Robocalls Are Even Worse Than You Thought](#) (May 15, 2019).
39. See Benjamin Siegel, Dr. Mark Abdelmalek, & Jay Bhatt, ABC News, [Coronavirus Contact Tracers' Nemeses: People Who Don't Answer Their Phones](#) (May 15, 2020). See also Stephen Simpson, [Few Picking Up Phone When Virus Tracers Call](#), Arkansas Democrat Gazette, July 10, 2020.
40. See Samantha Hawkins, Bloomberg Law, [Frontier Communications Sues Mobi Telecom Over Robocalls](#) (Feb. 9, 2022).
41. See Brian X. Chen, [Did You Receive a Text Message From Yourself? You're Not Alone](#), The N.Y. Times, Apr. 6, 2022.
42. See *id.* See also Verizon Community Forum, [Spam message from my own phone number?](#) (Mar. 27, 2022) (last visited Apr. 7, 2022).
43. See Federal Trade Comm'n, Consumer Advice, [How To Recognize and Report Spam Text Messages](#); Better Bus. Bureau, BBB Scam Alert: [Receive a text with a surprise offer? Don't click that link!](#) (Sept. 17, 2021); Better Bus. Bureau, BBB Tip: [Spot the red flags of fake text messages](#).
44. See AARP, Scams & Fraud, [Smishing](#).
45. FTC Consumer Sentinel Network, [Fraud Reports by Contact Method, Reports and Amount Lost by Contact Method](#) (updated Feb. 22, 2022) (Losses & Contact Methods tab, with years 2017 through 2021 checked). The data shows that 377,840 text scams were reported in 2021, and 90,939 in 2017. This is an increase of 286,901 complaints about scam texts, or 315%.
46. Federal Commc'ns Comm'n, [CGB—Consumer Complaints Data](#) (filtered for text messages for years 2017 and 2021). The 2017 data shows 6,093 complaints, and the 2021 data shows 14,835 complaints. This is an increase of 8,742 complaints about unwanted texts, or 143%. The FTC identifies scam texts as consumer fraud reports in which the consumer indicates that the contact method was text. See FTC Consumer Sentinel Network, [Fraud Reports by Contact Method](#) (updated Feb. 22, 2022).
47. FTC Consumer Sentinel Network, [Fraud Reports by Contact Method, Reports and Amount Lost by Contact Method, Year: 2021](#) (updated Feb. 22, 2022). The total amount of losses reported in complaints with the contact method of text message was \$37MM in 2017, and \$131MM in 2021. This is an increase of \$94MM, or 254%.
48. See *In re* Rules & Regulations Implementing the Tel. Consumer Prot. Act of 1991, Report & Order, CG Docket No. 02-278, 18 FCC Rcd. 14014, at ¶ 165 (F.C.C. July 3, 2003). *Accord In re* Rules & Regulations Implementing the Tel. Consumer Prot. Act of 1991, Declaratory Ruling and Order, CG Docket No. 02-078, WC Docket No. 07-135, 30 FCC Rcd. 7961, at ¶¶ 27, 107–108, 111–115 (F.C.C. July 10, 2015), appeal resolved, *ACA Int'l v. Federal Commc'ns Comm'n*, 885 F.3d 687 (D.C. Cir. 2018) (setting aside two parts of 2015 Declaratory Ruling, but leaving this portion undisturbed).
49. 47 U.S.C. § 227(a)(1)(A).
50. 47 C.F.R. §§ 64.1200(c)(2), 64.1200(f)(15) (definition of telephone solicitation; formerly numbered as 64.1200(f)(14) until the regulation was amended by 86 Fed. Reg. 2562 (Jan. 13, 2021)). See *Barton v. Temescal Wellness, L.L.C.*, 525 F. Supp. 3d 195 (D. Mass. 2021) (text message touting sellers' extended hours and including a link to its "menu" of goods and services was a solicitation). [The Do Not Call Registry can be found here.](#)
51. 592 U.S. ___, 141 S. Ct. 1163, 209 L. Ed. 2d 272 (2021).
52. NCLC and EPIC have articulated interpretations of the *Duguid* decision that cover many of the automated dialers currently in use. See National Consumer Law Center, Federal Deception Law § 6.3.4.1 (4th ed. 2022); Electronic Privacy Info. Ctr. (EPIC), Amicus Brief,

- [Evans v. Ocwen Loan Servicing, LLC, No. 21-14045](#) (11th Cir. Feb. 10, 2022); EPIC, Letter Brief, [Panzarella v. Navient Solutions, Inc., No. 20-2371](#) (3d Cir. Feb. 2, 2022); Amicus Brief, [Borden v. eFinancial, LLC, No. 21-35746](#) (9th Cir. Dec. 9, 2021).
53. 47 C.F.R. § 64.1200(f)(13). There is an additional legal theory that applies the TCPA's prohibition on prerecorded voices to text messages, but as of the time of this writing no court has recognized this theory. See *Eggleston v. Reward Zone USA, L.L.C.*, 2022 WL 886094 (C.D. Cal. Jan. 28, 2022).
 54. Federal Commc'ns Comm'n, [Report to Congress on Robocalls and Transmission of Misleading or Inaccurate Caller Identification Information](#) (Dec. 22, 2021) [hereinafter FCC 2021 Report to Congress]. See also Molly Sinclair, [Bell Pushes 25 Cents As Nationwide Pay-Phone Rate](#), *The Wash. Post.*, Dec. 14, 1981.
 55. FCC 2021 Report to Congress, *supra* note 54, at 12. See also Consumer Action, [1997 Long Distance Phone Rates Pricing Survey](#) (Feb. 1, 1997); Leslie Cauley, [Telephone Charges Creep Up Long-Distance Rates Rising After Years of Steady Drops](#), *The Baltimore Sun*, Mar. 27, 1992.
 56. FCC 2021 Report to Congress, *supra* note 54, at 12 n.61 (citing to Affidavit of Joshua M. Bercu, Vice President of Policy and Advocacy for USTelecom—The Broadband Association, at 1 (Dec. 2, 2020)).
 57. See Numbering Resources Report and Order, *supra* note 36, at ¶ 37. See also Farhan Chughtai, USTelecom, [Whitepaper: How to Identify and Mitigate Illegal Robocalls](#) 5 (Oct. 2019) at 5 [hereinafter *Identify and Mitigate Illegal Robocalls*].
 58. See, e.g., Federal Commc'ns Comm'n, FCC Fact Sheet, [Targeting Gateway Providers to Combat Illegal Robocalls](#) 45 ¶ 2(d) (Sept. 9, 2021) (defining gateway providers). See also *In re Advanced Methods to Target and Eliminate Unlawful Robocalls and Call Authentication Trust Anchor*, Fifth Further Notice of Proposed Rulemaking in CG Docket No. 17-59 & Fourth Further Notice of Proposed Rulemaking in WC Docket No. 17-97, CG Docket No. 17-59 and WC Docket No. 17-97, at ¶ 33 (Oct. 1, 2021), (proposing definition of gateway provider) [hereinafter Oct. 1, 2021 Notice of Proposed Rulemaking].
 59. See Numbering Resources Report and Order, *supra* note 36, at ¶ ¶ 33, 37, 47.
 60. Appendix to Complaint, *United States of America v. Palumbo*, Case 1:20-cv-00473, [Declaration of Marcy Ralston at 10-12 ¶ 22](#) (E.D.N.Y. Jan. 28, 2020) [hereinafter *Declaration of Marcy Ralston*] (“With modern telecommunications infrastructure, outbound VoIP calls do not take a defined path from their origin to the final destination. Rather, the system routes calls through automated equipment that determines the lowest possible connection cost at each routing step, depending on preexisting contractual relationships between the various entities. Typically, the company at each routing step will have numerous existing contracts through which it can route outbound calls through intermediate providers to the common carriers as the last routing step before an individual in the United States can answer the call. This automated routing process is called ‘least-cost routing.’”). Marcy Ralston, a Special Agent in the Social Security Administration’s Office of Inspector General, Office of Investigations, provided a sworn statement in *United States of America v. Palumbo*.
 61. See *id.*
 62. See FCC 2021 Report to Congress, *supra* note 54, at 12 (“The Commission’s experience tracing back the origins of unlawful call traffic indicates that a disproportionately large number of calls originate from Voice over Internet Protocol (VoIP) providers, particularly non-interconnected VoIP providers. Moreover, the Industry Traceback Group has found that high-volume, rapid-fire calling is a cost-effective way to find susceptible targets, although it does not collect data about which robocall originators are VoIP providers.”).

63. See, e.g., Oct. 1, 2021 Notice of Proposed Rulemaking, *supra* note 58, at ¶ 33.
64. See Declaration of Marcy Ralston *supra* note 60, at 10 ¶ 20.
65. *Id.*
66. See *id.* at 12-13 ¶ 24 (“Those records further demonstrate that since at least 2016, Nicholas and Natasha Palumbo have operated TollFreeDeals as a VoIP carrier, originally out of their home in Scottsdale, Arizona, and since mid-2019 out of their current home in Paradise Valley, Arizona.”); Ryan Tracy & Sarah Krouse, *Where Robocalls Hide: the House Next Door*, *The Wall St. J.*, Aug. 15, 2020 (“Mr. Palumbo accumulated more than \$3.2 million on the hundreds of millions of calls routed through a telecom operation based in his Paradise Valley, Ariz., home last year.”).
67. See *In re Matters of IP-Enabled Services et al.*, Order, WC Docket No. 04-36 et al., at ¶ 6 n.19 (Rel. Oct. 9, 2007) (a VoIP service is “nomadic” if it can be used from multiple locations). A nomadic VoIP service provider can still be an interconnected VoIP provider. *In re Matters of IP-Enabled Services et al.*, Order, WC Docket No. 04-36 et al., at ¶ 3 n.8 (Rel. Apr. 4, 2008).
68. See AT&T Business, [What is VoIP and how does it work?](#).
69. See Xfinity, [What is Voice Over Internet Protocol?](#)
70. An “interconnected VoIP service” is a service that “(i) [e]nables real-time, two-way voice communications; (ii) [r]equires a broadband connection from the user’s location; (iii) [r]equires internet protocol-compatible customer premises equipment (CPE); and (iv) [p]ermits users generally to receive calls that originate on the public switched telephone network and to terminate calls to the public switched telephone network.” 47 C.F.R. § 9.3. See *also* 47 U.S.C. § 153(25) (incorporating this definition by reference).
71. See Declaration of Marcy Ralston, *supra* note 60, at 10 ¶ 22 (“Tracebacks of many different robocalling fraud schemes have led to the identification of Defendants as a gateway carrier willing to transmit huge volumes of fraudulent robocalls into the country, despite clear indicia of fraud in the call traffic and actual notice of fraud.”).
72. [Complaint, State of Vermont v. Bohnett](#), Case No. 5:22-cv-00069, at 9 ¶ 37 (D. Vt. Mar. 18, 2022) [hereinafter Vermont Complaint].
73. See *id.* at 9 ¶ 34.
74. According to the Industry Traceback Group, 50% of identified illegal robocalls originated in the United States. Industry Traceback Group, [Combatting Illegal Calls: ITG By the Numbers](#). See *also In re Advanced Methods to Target and Eliminate Unlawful Robocalls et al.*, CG Docket No. 17-59 et al., Reply Comments of Verizon at 10 (filed Jan. 10, 2022) (observing that “bad actors would simply place more intermediate other service providers between themselves and the gateway provider, making it impossible for the gateway provider to identify and consistently stop the illegal traffic”).
75. See Vermont Complaint, *supra* note 72, at 9 ¶ 34.
76. See *id.* at 9 ¶ 35.
77. See FCC 2021 Report to Congress, *supra* note 54, at 12-13 (“Short-duration calls became popular after providers introduced six-second billing as an alternative to rounding up, as a way to become more competitive with other providers. This approach made short duration calls much less expensive, leading to a cottage industry of VoIP providers specializing in ‘dialer traffic.’ These providers compete with each other on thin margins, often with minimal staff, rented servers, online sign-ups, and virtual offices, to generate high volumes of calls. . . .”). See *also id.* at 13 n.64 (citing to [Combatting Robocall Fraud: Using Telecom Advances and Law Enforcement to Stop Scammers and Protect Seniors](#), Hearing Before the Senate Special Committee on Aging, 116th Cong. (July 17, 2019) ([written testimony of David](#)

Frankel, CEO, ZipDX LLC, at 3) (describing “small operations—a few dozen people or perhaps just one or two” that “[b]lend in robocall traffic with their other business” to supplement their bottom line)).

78. See [Great Choice Telecom](#) (ANI/ DID/CID rotator feature claims to “provide you a hands free system for Caller ID’s to change after every call made, engineered to help have more connected calls as well as stay away from scam likely”). On February 10, 2022, the FCC issued a cease and desist letter to Great Choice Telecom, requiring the provider to take mitigation steps within 48 hours and within 14 days. [Letter from FCC to Mikel Quinn, CEO of Great Choice Telecom](#) (Feb. 10, 2022). As of February 28, 2022, that language still appeared on its [website](#), and also as of May 20, 2022.
79. [Automated Number Identification \(ANI\)](#) is a form of caller ID. See *also* [Complaint for Injunctive Relief and Civil Penalties](#), North Carolina *ex rel.* Stein v. Articul8, LLC & Paul K. Talbot, Case No. 1:22-cv-00058, at 16 ¶ 60 (M.D.N.C. Jan. 25, 2022) [hereinafter Articul8 Complaint].
80. See Articul8 Complaint, *supra* note 79, at 17 ¶ 61.
81. See *id.* at 16 ¶ 60 (“For example, a legitimate telemarketer making 100,000 calls across five campaigns would typically use five different ANIs with an average of 20,000 calls per ANI. Among other things, using a single ANI for each campaign allows a legitimate telemarketer to track metrics associated with calling campaigns for different services or companies.”). See *also id.* at 18 ¶ 65 (“The average Calls-Per-ANI of [Defendant’s] calls was 1.08, which means that almost every one of the over 4.4 million calls answered came from a distinct—and likely illegally spoofed—calling number.”).
82. Declaration of Marcy Ralston, *supra* note 60, at 9 ¶ 19 (“Foreign call centers and VoIP carriers cannot connect VoIP phone traffic directly to the U.S. telephone system from a foreign location without the assistance of a U.S.-based telecommunications provider willing to accept the foreign call traffic.”). See *also* [United States v. Palumbo](#), 448 F. Supp. 3d 257, 265 (E.D.N.Y. 2020) (“the telecommunications ‘intermediary’ industry is set up perfectly to allow fraudulent operators to rotate telephone numbers endlessly and blame other parties for the fraudulent call traffic they carry”).
83. See TRACED Act, Pub. L. No. 116-105, § 13(d), 133 Stat. 3274 (2019).
84. *In re Implementing Section 13(d) of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act* (TRACED Act), Report and Order, EB Docket No. 20-22, at ¶ 1 (Aug. 25, 2021).
85. See *id.* See *also* <https://www.ustelecom.org/ustelecom-community/>.
86. See Vermont Complaint, *supra* note 72, at 12 ¶ 52.
87. [Industry Traceback Group, Policies and Procedures 8](#) (revised July 2021) [hereinafter ITG Policies and Procedures].
88. See *id.*
89. See *id.*
90. Vermont Complaint, *supra* note 72, at 13 ¶ 54.
91. See Industry Traceback Group, [2021 ITG Combatting Illegal Robocalls Report 6](#) [hereinafter 2021 ITG Report]. See *also* ITG By the Numbers, *supra* note 74.
92. Letter from Joshua M. Bercu and Jessica Thompson, USTelecom, to Marlene Dortch, Federal Commc’ns Comm’n, [Enforcement Bureau Requests Information on the Status of Private-Led Traceback Efforts of Suspected Unlawful Robocalls](#), EB Docket No. 20-195 (filed Nov. 15, 2021) [hereinafter Bercu and Thompson Letter].
93. Articul8 Complaint, *supra* note 79, at 12 ¶ 42. See *also* Vermont Complaint, *supra* note 72, at 14 ¶ 57.

94. See Vermont Complaint, *supra* note 72, at 13 ¶ 53.
95. See Articul8 Complaint, *supra* note 79, at 12 ¶ 42.
96. Each traceback notice sent to every provider in the call path contains a text description of the call, typically explaining what makes it illegal. See *id.* at 30 ¶¶ 93-94 and 34 ¶¶ 98-99. In addition, most traceback notices include a link to the recorded message that was captured. North Carolina alleged that ITG notified Articul8 of this illegal traffic 49 times for calls. *Id.* at 30 ¶ 93. In one version of the Social Security scam, “the caller says your Social Security number has been linked to a crime (often, he says it happened in Texas) involving drugs or sending money out of the country illegally.” Jennifer Leach, Federal Trade Comm’n, Consumer Advice, [Fake calls about your SSN](#) (Dec. 12, 2018).
97. See Complaint for Civil Penalties, Permanent Injunction, Other Equitable Relief, and Demand for Jury Trial, *Indiana v. Startel Commc’n L.L.C.*, No. 3:21-cv-00150, 2021 WL 4803899, at ¶ 314 (S.D. Ind. Oct. 14, 2021) (“On July 22, 2020, Piratel’s CEO responded to the email, writing: ‘We will need to review internally and with USTelecom as to if we are willing to enable your trunk again. We have received 4 tracebacks in 3 weeks which is the most tracebacks we have received from any single customer, much less in the space of time.’”) [hereinafter Startel Complaint]. See also *id.* at ¶ 316 (“Despite receiving four Tracebacks, which alerted them of illegal robocalls, Piratel did not terminate Startel as a client. Quite the opposite, Startel went on to route millions more calls to Hoosiers through Piratel’s system, and Piratel continued to collect thousands of dollars from Startel.”). As a result of Indiana’s lawsuit, Piratel signed a consent decree requiring the payment of \$150,000 over five years, as well as injunctive relief including network monitoring, a prohibition on providing services to new Voice Service Provider (VSP) Customers without first engaging in reasonable screening, and the suspension of service to VSP Customers failing to meet certain requirements—without Piratel admitting fault. See Consent Decree, *Indiana v. Startel Commc’n L.L.C.*, No. 3:21-cv-00150 (Apr. 6, 2022).
98. See Articul8 Complaint, *supra* note 79, at 30 ¶ 94. In the Vermont Attorney General’s case against a gateway provider known as TCA VOIP, the defendant had been the recipient of an astonishing 132 traceback requests. See Vermont Complaint, *supra* note 72, at 17 ¶ 79.
99. See [Gartner Glossary, Call Detail Record \(CDR\)](#).
100. See [Re: Notice of Ex Parte Presentation by National Consumer Law Center, EPIC, Consumer Reports, National Consumers League, U.S. PIRG, and Public Knowledge to FCC Staff](#), EC Docket No. 17-97, Call Authentication Trust Anchor; CG Docket No. 17-59, Advanced Methods to Target and Eliminate Unlawful Robocalls, at 4 (filed Feb. 10, 2022).
101. Articul8 Complaint, *supra* note 79, at 18 ¶ 65.
102. See, e.g., *id.* at 3 ¶ 4.
103. See, e.g., TB Wiki, [Text Call Detail Records](#). See also CFCa KNOW Webinar, [Robocall Mitigation, What Can You Do to Prevent Illegal Robocalling?](#), at 8:00, 11:49 (Mar. 28, 2022).
104. Vermont Complaint, *supra* note 72, at 33 ¶ 123 (“Despite the Vermont Attorney General requesting TCA VOIP to place a litigation hold on CDRs during this investigation, TCA VOIP is deliberately allowing its CDRs during the investigation to be destroyed as part of a very short retention policy. As the Vermont Attorney General got better, faster access to traceback data, TCA VOIP advised its switch or software provider on January 10, 2022: ‘The AG’s have gotten faster. The latest request is for Dec 13th forward. Can you verify that the oldest is rolling off and I have 90 days of data?’”).
105. The Vermont AG based its case against TCA VOIP in part upon content analytics. See Vermont Complaint, *supra* note 72, at ¶¶ 109-11, 117 (call detail records indicating high likelihood of fraud, due to content such as “This call is from a federal agency to suspend

your social security number on an immediate basis. As we have received suspicious trails of information with your name. The moment you receive this message. You need to get back to us to avoid the consequences to connect the call immediately press one.”).

106. See, e.g., Gerry Christensen, LinkedIn, [Content-based Analytics Definitively Identifies Fraudulent Robocalls](#) (Sept. 23, 2021).
107. Electronic Privacy Information Center cautions against over-reliance on content analytics as a robocall mitigation policy, as it could lead to a regime wherein all voice messages are monitored, with or without the consumer’s knowledge.
108. *In re Call Authentication Trust Anchor, Further Notice of Proposed Rulemaking*, WC Docket No. 17-97 (Sept. 30, 2021) (Statement of Comm’r Geoffrey Starks) [hereinafter Statement of Comm’r Geoffrey Starks].
109. See CTIA, [Messaging Principles and Best Practices 15](#) (July 2019).
110. Campaign Registry, [About The Campaign Registry](#).
111. See Emily Champion, [Bandwidth Support Center, 10 DLC Overview](#) (updated Mar. 2022). Compare \$0.003 per message for registered traffic with \$0.004 per message for unregistered traffic at T-Mobile, and \$0.004 for unregistered and \$0.002 for registered at AT&T.
112. See *id.* Compare \$0.002 for political messaging with \$0.003 for insurance agents.
113. See also *Barr v. Am. Ass’n of Political Consultants, Inc.*, ___ U.S. ___, 140 S. Ct. 2335, 2344, 207 L. Ed. 2d 784 (2020) (Congress’s enactment of the TCPA “followed a torrent of vociferous complaints about intrusive robocalls. . . . Consumers were ‘outraged’ and considered robocalls an invasion of privacy. . . . In enacting the TCPA, Congress found that banning robocalls was ‘the only effective means of protecting telephone consumers from this nuisance and privacy invasion.’ ”); S. Rep. No. 102-178, at 5 (1991), reprinted in 1991 U.S.C.C.A.N. 1968, 1972–1973 (“The Committee believes that Federal legislation is necessary to protect the public from automated telephone calls. These calls can be an invasion of privacy, an impediment to interstate commerce, and a disruption to essential public safety services.”).
114. TRACED Act, Pub. L. No. 116-105, 133 Stat. 3274 (2019).
115. YouMail estimated that there were over 45.8 billion robocalls placed in 2020 and 50.5 billion calls placed in 2021. YouMail, [Historical Robocalls By Time](#). YouMail estimated that 46% of robocalls in 2020, or 21.1 billion, were scam robocalls. PR Newswire, [Americans Hit by Just Under 46 Billion Robocalls in 2020, Says YouMail Robocall Index](#) (Jan. 26, 2021). YouMail estimated that 42% of robocalls in 2021, or 21.2 billion, were scam robocalls. PR Newswire, [U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#) (Jan. 6, 2022).
116. Since June 2019, the FCC has permitted (but not required) callers to block calls likely to be illegal. See Press Release, Federal Commc’ns Comm’n, [FCC Affirms Robocall Blocking by Default](#) (June 6, 2019) (“Specifically, the Commission approved a Declaratory Ruling to affirm that voice service providers may, as the default, block unwanted calls based on reasonable call analytics, as long as their customers are informed and have the opportunity to opt out of the blocking.”). Since March 2020, the FCC has stated that it expects providers’ use of call analytics supplementing STIR/SHAKEN to be sufficient to stem the tide of illegal robocalls. See Numbering Resources Report and Order, *supra* note 36, at ¶ 25 (“we expect STIR/SHAKEN paired with call analytics to serve as a tool to effectively protect American consumers from fraudulent robocall schemes”). Despite the statistical evidence of the shortcomings of these regulatory approaches, recent rulemaking proposals largely advance similar strategies. See, e.g., Oct. 1, 2021 Notice of Proposed Rulemaking, *supra* note 58, at ¶ 61 (proposing that downstream providers be required to block illegal calls only after

notification from the Commission). *But see id.* at ¶ 66 (proposing that only gateway providers be required to block calls highly likely to be illegal based on analytics), at ¶ 92 (proposing the imposition of a general duty only on gateway providers to take affirmative, effective measures rather than merely reasonable steps to combat robocalls).

117. Federal Commc'ns Comm'n, Sixth Report and Order, Seventh Further Notice of Proposed Rulemaking—CG Docket No. 17-59, [Fifth Report and Order, Order on Reconsideration, Fifth Further Notice of Proposed Rulemaking](#)—WC Docket No. 17-97 (Rel. May 20, 2022) [hereinafter Sixth Report and Order] (including a 24-hour response period for tracebacks, requiring blocking similar traffic but only upon notification from the FCC, requiring a “reasonable” Do Not Originate (DNO) List but not imposing minimum requirements and imposing limits on the scope, and holding Gateway Providers to a “reasonable steps” but not an “effective measures” standard in their robocall mitigation plans).
118. *See, e.g., In re Advanced Methods to Target and Eliminate Unlawful Robocalls*, Report and Order and Further Notice of Proposed Rulemaking, CG Docket No. 17-59, 32 FCC Rcd. 9706, at ¶¶ 9-56 (Rel. Nov. 17, 2017). The Commission also allowed providers to block all calls not on a consumer’s whitelist, which was on an opt-in basis. *Id.* at ¶¶ 26-42.
119. *In re Advanced Methods to Target and Eliminate Unlawful Robocalls*, [Fourth Report and Order](#), CG Docket No. 17-59, FCC 20-187, at ¶¶ 39-47 (Rel. Dec. 30, 2020).
120. *See* Section III.A, *supra*.
121. *See* FCC 2021 Report to Congress, *supra* note 54, at 9; 47 C.F.R. §§ 64.6301 to 64.6304 (requiring originating providers to either implement the STIR/SHAKEN technology on their network or, if unable, to implement another robocall mitigation technology by June 30, 2021, with additional time for certain categories of voice service providers that face undue hardship; also requiring intermediate providers and terminating providers to pass along the caller ID authentication information without alteration, with two narrow exceptions); *In re Call Authentication Trust Anchor*, [Fourth Report and Order](#), WC Docket No. 17-97, FCC 21-122 (Rel. Dec. 10, 2021) (shortening the additional time to comply for those providers likely to be the source of illegal calls); Federal Commc'ns Comm'n, Call Authentication Trust Anchor, Final Rule, 85 Fed. Reg. 73660 (Nov. 17, 2020).
122. *See* TransNexus, [Understanding STIR/SHAKEN](#).
123. A call is given a “Full Attestation (A)” when the voice service provider knows that the caller is authorized to use the calling number. “Partial Attestation (B)” means that the service provider knows the call source, but cannot verify that the caller is authorized to use the calling number. “Gateway Attestation (C)” means that the service provider knows where the call came from (i.e. either the caller, or the provider who passed the call to this provider), but cannot authenticate the call source. An example of this case would be a call received from an international gateway. *See id.* For more information on attestation, see NANC Call Authentication Trust Anchor Working Group, [Best Practices for the Implementation of Call Authentication Frameworks](#) 5, 23, and Numbering Resources Report and Order, *supra* note 36, at ¶ 8.
124. TransNexus has claimed that a greater percentage of robocalls may receive level B attestation than receive no attestation at all. *See* TransNexus, [Spam robocalls and SHAKEN attestation](#) (July 26, 2021). YouMail and Hiya have indicated that even an attestation is imperfect. *See* What Everyone Needs to Know, *supra* note 23, at slide 5 (Mar. 21, 2022); Hiya, Unexpected Effects of STIR/SHAKEN, presentation at SIPNOC 2022 Webinar Series, at slide 22 (Mar. 21, 2022).
125. *See* FCC 2021 Report to Congress, *supra* note 54, at 9; 47 C.F.R. § 64.6305(b).
126. *See* FCC 2021 Report to Congress, *supra* note 54, at 9; 47 C.F.R. §§ 64.6301 to 64.6304

- (requiring originating providers to either implement the STIR/SHAKEN technology on their network or, if unable, to implement another robocall mitigation technology by June 30, 2021).
127. *In re Call Authentication Trust Anchor, Fourth Report and Order*, WC Docket No. 17-97, FCC 21-122 (Rel. Dec. 10, 2021) (shortening the additional time to comply for those providers likely to be the source of illegal calls).
 128. See FCC 2021 Report to Congress, *supra* note 54, at 9; 47 C.F.R. § 64.6305(b).
 129. The FCC has threatened to remove non-compliant providers from the RMD on an ad hoc basis. See, e.g., [Letter from FCC Enforcement Bureau to Dominic Bohnett, CEO of Telecom Carrier Access, Inc. dba TCA Voip](#) (Feb. 10, 2022) (“downstream voice service providers will be authorized to **block all** of TCA Voip’s traffic if you do not take steps to ‘effectively mitigate illegal traffic’ within 48 hours, or if you fail to inform the Commission and the Traceback Consortium within fourteen (14) days of this letter (Thursday, February 24, 2022), of the steps you have taken to ‘implement effective measures’ to prevent customers from using your network to make illegal calls.” (emphasis in original)). However, as of the time of this writing, the Commission has never publicly announced that it removed a provider. For a list of providers who have recently received these letters, see Press Release, Federal Commc’ns Comm’n, [FCC Continues to Send Cease-And-Desist Letters to Voice Service Providers Suspected of Facilitating Illegal Robocalls](#) (Feb. 17, 2022) [hereinafter FCC Continues to Send Cease-And-Desist Letters].
 130. John Spiller, along with other individual and corporate defendants, was assessed the largest fine in FCC history in June 2020 for his role in spoofing phone numbers, calling numbers on the Do Not Call registry, and calling wireless phones without first obtaining consumer consent. See Press Release, Federal Commc’ns Comm’n, [Health Insurance Telemarketer Faces Record FCC Fine of \\$225 Million for Spoofed Robocalls](#) (Mar. 17, 2021). Biographical information about John Spiller was included on the About Us page of Great Choice Telecom, but this page has since been taken down. However, at the time of this writing, [very similar information is provided here](#). The contact information for these two organizations is identical, including the phone number and the suite number. *Compare* <https://web.archive.org/web/20220330212507/https://aroadtochrist.org/about-us/> with <https://web.archive.org/web/20220228151117/greatchoicetelecom.com/>. The FCC sent a cease and desist letter to Great Choice Telecom in early 2022, but did not reference [John Spiller. Letter from FCC to Mikel Quinn, CEO of Great Choice Telecom](#) (Feb. 10, 2022). As this report went to print, the FCC proposed several changes to address new registrations from known bad actors. See Sixth Report and Order at ¶ 207, *supra* note 117. However, even if all of these proposals are adopted, they will not trigger automatic suspension or de-certification.
 131. See TRACED Act, Pub. L. No. 116-105, § 13(d), 133 Stat. 3274 (2019).
 132. See ITG Policies and Procedures, *supra* note 87 at 8.
 133. See FCC 2021 Report to Congress, *supra* note 54, at 16.
 134. See ITG Report, *supra* note 91, at 12; Bercu and Thompson Letter, *supra* note 92. See also ITG By the Numbers, *supra* note 74.
 135. See [Letter from FCC Enforcement Bureau to Aaron Leon, Co-Founder & CEO of thinQ Technologies, Inc.](#) (Mar. 22, 2022).
 136. See [Letter from FCC Enforcement Bureau to Vitaly Potapov, CEO, RSCOM LTD](#) (May 20, 2020).
 137. See [Letter from FCC Enforcement Bureau to Karl Douthit, CEO, Piratel, L.L.C.](#) (Feb. 4, 2020); Startel Complaint, *supra* note 97.
 138. Federal Commc’ns Comm’n, [FCC Enforcement Bureau Writes Gateway Providers on](#)

[Robocall Traceback](#) (Rel. Feb. 4, 2020); Press Release, Federal Trade Comm'n, [Globex Telecom and Associates Will Pay \\$2.1 Million, Settling FTC's First Consumer Protection Case Against a VoIP Service Provider](#) (Sept. 22, 2020).

139. See FCC 2021 Report to Congress, *supra* note 54, at Attachment A. Compare Participating tab (including all four providers listed above, as well as AT&T and Verizon) and Non-Responsive tab (containing none of the four providers listed above). See also Federal Commcn's Comm'n, [Report to Congress on Robocalls and Transmission of Misleading or Inaccurate Caller Identification Information](#) (Dec. 23, 2020) (including 2019 enforcement actions in its 2020 report).
140. See FCC 2021 Report to Congress, *supra* note 54, at 16.
141. See ITG Report, *supra* note 91, at 12; Bercu and Thompson Letter, *supra* note 92. See also ITG By the Numbers, *supra* note 74.
142. See Federal Commc'ns Comm'n, [Robocall Facilitators Must Cease and Desist](#) [hereinafter Robocallers Must Cease and Desist].
143. See Articul8 Complaint, *supra* note 79, at 30 ¶¶ 94.
144. See Vermont Complaint, *supra* note 72, at 17 ¶¶ 79.
145. 47 C.F.R. § 64.1200(n)(1), *adopted by* Federal Commc'ns Comm'n, [Advanced Methods to Target and Eliminate Unlawful Robocalls, Final Rule](#), 86 Fed. Reg. 17,726, 17,727, 17,735 (Apr. 6, 2021). ("All voice service providers must . . . respond fully and in a timely manner to all traceback requests from certain entities"). Yet, no enforcement actions have been taken to date addressing a failure to comply with traceback requests. See Robocallers Must Cease and Desist, *supra* note 142.
146. Oct. 1, 2021 Notice of Proposed Rulemaking, *supra* note 58, at ¶¶ 2. The FCC also stated: "Driven in part by the rise of VoIP, the telecommunications industry has transitioned from a limited number of carriers that all trusted each other to provide accurate calling party origination information to a proliferation of different voice service providers and entities originating calls, which . . . creates new ways for bad actors to undermine trust." *Id.* The FCC cited the TRACED Act, noting that "[s]ection 6(a) of the TRACED Act also requires the Commission to 'commence a proceeding to determine how Commission policies regarding access to number resources, including number resources for toll-free and non-toll-free telephone numbers, could be modified, including by establishing registration and compliance obligations, and requirements that providers of voice service given access to number resources take sufficient steps to know the identity of the customers of such providers' within 180 after enactment." *Id.* at ¶ 2 n.1. See also Numbering Resources Report and Order, *supra* note 36, at ¶¶ 123-130.
147. TRACED Act, Pub. L. No. 116-105, § 6, 133 Stat. 3274 (2019).
148. 47 C.F.R. § 64.1200(n)(3), *added by* Federal Commc'ns Comm'n, [Advanced Methods to Target and Eliminate Unlawful Robocalls, Final Rule](#), 86 Fed. Reg. 17,726, 17,727, 17,735 (Apr. 6, 2021).
149. FCC 2021 Report to Congress, *supra* note 54, at 13 (citing *In re* Numbering Policies for Modern Communications et al., WC Docket No. 13-97 et al., Further Notice of Proposed Rulemaking, FCC 21-94, at ¶ 13 (Rel. Aug. 6, 2021) and the TRACED Act § 6(a)(1)).
150. *Id.* (citing *In re* Numbering Policies for Modern Communications et al., WC Docket No. 13-97 et al., Further Notice of Proposed Rulemaking, FCC 21-94, at ¶ 14 (Rel. Aug. 6, 2021)).
151. Oct. 1, 2021 Notice of Proposed Rulemaking, *supra* note 58. As this report went to print, the FCC adopted regulations requiring gateway providers to "know" their immediate upstream foreign provider. See Sixth Report and Order at ¶ 96, *supra* note 117. The problem with this new FCC requirement is that even for a gateway provider that "repeatedly allows a high

volume of illegal traffic onto the U.S. network,” the provider is only required to change its approach. Yet there does not appear to be sufficient incentives to ensure that the gateway will employ effective methodologies.

152. *id.* at ¶¶ 60-61. The Commission also proposed requiring providers to respond to tracebacks within 24 hours, mandatory call blocking (after receiving notice from the Commission), Know Your Customer provisions, and contractual provisions regarding mitigation (¶ 40), as well as a general mitigation standard that demands “reasonable steps” rather than effective measures (¶ 91), and certification in the RMD (¶ 94) (describing their robocall mitigation practices and stating that they are adhering to those practices). (See “Establishing the Robocall Mitigation Database” in point #4 of this section for why this last proposal is unlikely to impact robocalls.) This appears to be unchanged in the Commission’s May 20 order. See Sixth Report and Order, *supra* note 117.
153. See *What Everyone Needs to Know*, *supra* note 23. This appears to be unchanged in the Commission’s May 20th Order. See Sixth Report and Order, *supra* note 117.
154. See, e.g., <https://greatchoicetelecom.com/> (Great Choice Telecom advertises rotating ANIs).
155. See Federal Comm’n’s Comm’n, *Numbering Policies for Modern Communications*, Proposed Rules, WC Docket Nos. 13-97, 07-243, 20-67, IB Docket No. 16-155, 86 Fed. Reg. 51,081 (Sept. 14, 2021).
156. *Id.* at ¶ 4.
157. This is similar to the proposal made by USTelecom. See *Identify and Mitigate Illegal Robocalls*, *supra* note 57, at 8, 9.
158. Five in its 2020 report to Congress, plus one unique addition in 2021. See Federal Comm’n’s Comm’n, [Report to Congress on Robocalls and Transmission of Misleading or Inaccurate Caller Identification Information](#) (Dec. 23, 2020) (including 2019 enforcement actions in its 2020 report); FCC 2021 Report to Congress, *supra* note 54.
159. See 2021 ITG Report, *supra* note 91. See also *ITG By the Numbers*, *supra* note 74.
160. See *Robocallers Must Cease and Desist*, *supra* note 142.
161. See *In re* John C. Spiller; Jakob A. Mears; Rising Eagle Capital Group LLC; JSquared Telecom LLC; Only Web Leads LLC; Rising Phoenix Group; Rising Phoenix Holdings; RPG Leads; and Rising Eagle Capital Group—Cayman, Notice of Apparent Liability for Forfeiture, 35 FCC Rcd. 5948 (June 10, 2020).
162. See *FCC Continues to Send Cease-And-Desist Letters*, *supra* note 129. See also note 130, *supra*, for information about Spiller’s apparent involvement with Great Choice Telecom.
163. 16 C.F.R. § 310, as amended by 68 Fed. Reg. 4580 (Jan. 29, 2003). Issued pursuant to the Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. §§ 6101 to 6108.
164. 16 C.F.R. § 310.3(b). See, e.g., *Federal Trade Comm’n v. Educare Ctr. Servs., Inc.*, 433 F. Supp. 3d 1008, 1017 (W.D. Tex. 2020). See also *Federal Trade Comm’n v. Affiliate Strategies, Inc.*, 714 F.3d 1211 (10th Cir. 2013) (writer of grant guide provided substantial assistance to fraudulent telemarketer of grant-finding services; drafted talking points for telemarketers, dealt with customer complaints, but never followed up to determine whether anyone actually received a grant); *Federal Trade Comm’n v. Partners In Health Care Ass’n, Inc.*, 189 F. Supp. 3d 1356 (S.D. Fla. 2016) (finding company that sold medical discount card and its principal liable for telemarketers’ misrepresentations; company processed all payments, fulfilled customer orders, and opened telemarketers’ merchant accounts, and principal reviewed telemarketers’ materials and handled complaints); *United States v. DISH Network, L.L.C.*, 75 F. Supp. 3d 942 (C.D. Ill. 2014) (fact question whether defendant seller of satellite TV services knew or consciously avoided knowing about one co-defendant retailer’s TSR violations; knowledge or conscious avoidance not shown as to other

retailers), *vacated in part*, 80 F. Supp. 3d 917 (C.D. Ill. 2015), *aff'd in part, vacated in part on other grounds*, 954 F.3d 970 (7th Cir. 2020); Federal Trade Comm'n v. HES Merch. Servs. Co., 2014 WL 6863506 (M.D. Fla. Nov. 18, 2014) (finding individual liability based on owner's awareness of probable fraud and intentional avoidance of the truth), *aff'd, vacated in part on other grounds*, 652 Fed. Appx. 837 (11th Cir. 2016). See also Fed. Trade Comm'n v. Global Mktg. Grp., Inc., 594 F. Supp. 2d 1281 (M.D. Fla. 2008) (U.S.-based principal whose companies processed payments for Canadian advance-fee credit-card telemarketers, fulfilled orders, handled complaints, negotiated agreements with merchants, and provided other assistance is liable for telemarketers' fraud).

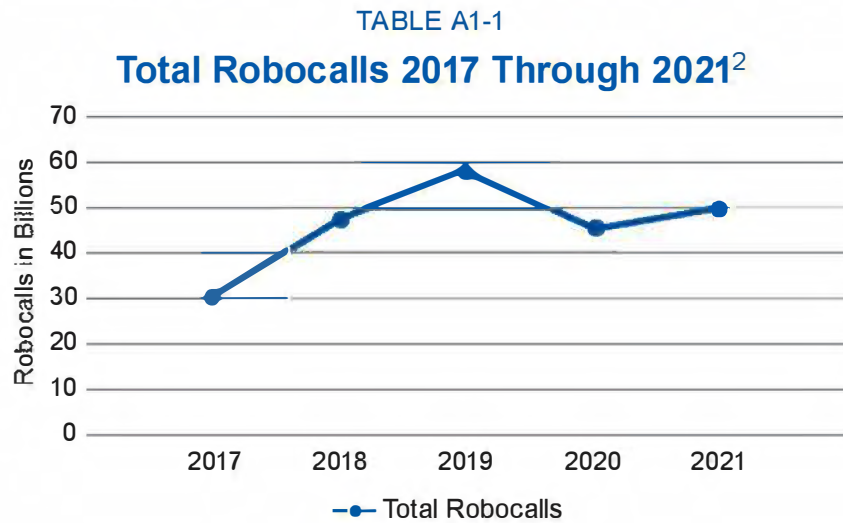
165. Federal Trade Comm'n v. Consumer Health Benefits Ass'n, 2011 WL 3652248, at *10 (E.D.N.Y. Aug. 18, 2011).
166. See, e.g., Press Release, Federal Trade Comm'n, [FTC to VoIP Providers: Turn over Information for Robocall Investigations or Prepare to be Sued in Federal Court](#) (Feb. 14, 2022).
167. See, e.g., Press Release, Federal Trade Comm'n, [FTC Takes Action against Second VoIP Service Provider for Facilitating Illegal Telemarketing Calls](#) (Dec. 3, 2020); Press Release, Federal Trade Comm'n, [Globex Telecom and Associates Will Pay \\$2.1 Million, Settling FTC's First Consumer Protection Case Against a VoIP Service Provider](#) (Sept. 22, 2020).
168. Press Release, Federal Trade Comm'n, [FTC Warns 19 VoIP Service Providers That 'Assisting and Facilitating' Illegal Telemarketing or Robocalling Is Against the Law](#) (Jan. 30, 2020).
169. Lesley Fair, [Telemarketing Sales Rule: We asked. You answered. We heard you.](#) (Apr. 28, 2022); Federal Trade Comm'n, [16 CFR 310: Telemarketing Sales Rule; Notice of Proposed Rulemaking](#) (Apr. 28, 2022); Federal Trade Comm'n, [16 Part 310: Telemarketing Sales Rule; Advanced Notice of Proposed Rulemaking](#) (Apr. 28, 2022).
170. Licensing and bonding requirements can ensure that even smaller providers can make defrauded consumers whole. See Section V, proposal 5, *infra*.
171. See, e.g., [Anti-Robocall Principles for Voice Service Providers, Principles #3 and #4](#) (2019) (statement signed by 51 state attorneys general and twelve telecommunications providers, committing to a set of principles that explicitly include requiring providers to monitor traffic on their networks and investigate suspicious patterns, and urging that providers who suspect that illegal robocalling or spoofing is occurring through their network verify that the originating commercial customer owns or is authorized to use the caller ID number, determine whether the caller ID sent matches the customer's name, terminate the party's ability to originate, route, or terminate calls, and notify law enforcement authorities); [Identify and Mitigate Illegal Robocalls](#), *supra* note 57, at 8-9 (charging originating providers with responsibility to take action where evidence suggested illegal robocalling occurred, and similarly emphasizing that downstream providers should be considered responsible for taking action when originating provider has failed to do so; urging originating providers to impose network level constraints; suggesting discontinuance of service for ongoing violations; urging FCC to require downstream providers to be alert to indicators of illegal activities and refuse to process calls from violators); [In re Advanced Methods to Target and Eliminate Unlawful Robocalls, Comments of Comcast Corporation, CG Docket 17-59 and WC Docket No. 17-97](#), at 3 (filed Dec. 10, 2021) ("while gateway providers' current obligations to respond to traceback requests and to respond to Commission notifications of unlawful traffic are significant and beneficial, they are largely *reactive* in nature, and cannot take the place of *proactive* duties to mitigate harmful traffic directed towards the United States from abroad" (emphasis in original)).

172. 47 C.F.R. § 64.1200(k)(4).
173. 47 C.F.R. § 64.1200(k)(3).
174. 47 C.F.R. § 64.1200(n)(2).
175. 47 C.F.R. §§ 64.1200(n)(3), (4) & (5). However, these providers are still permitted to continue to transmit calls into the network, until they receive notice from the Commission to stop.
176. Statement of Comm'r Geoffrey Starks, *supra* note 108.
177. The Truth in Lending Act precludes a credit card issuer from imposing liability on a customer (business or consumer) for unauthorized use of a credit card, except in narrowly defined circumstances. 15 U.S.C. § 1643.
178. See Section III, *supra* (discussing these analytics).
179. USTelecom recommended that downstream providers should be required to notify offending Originating Providers of “terms-of-service and/or acceptable-use-policy violations,” but without financial incentives these measures are likely to be inadequate. Identify and Mitigate Illegal Robocalls, *supra* note 57, at 8.
180. Suspension should result in legally effective removal from the RMD, but not physical removal. Rather, suspension should entail a prominent notation that the provider’s status is suspended. See, e.g., *In re Advanced Methods to Target and Eliminate Unlawful Robocalls et al., Comments of ZipDX L.L.C., CG Docket No. 17-59 and WC Docket No. 17-97*, at 24 (filed Dec. 7, 2021) (“We would note that ‘delisting’ should not actually constitute complete removal from the database; rather, an entry should be retained so that it is clear to all others that the problematic provider has been explicitly designated as such. This will ensure that if (when) the problematic provider attempts to shift their traffic to a new downstream, that downstream will become aware of the situation before enabling the traffic.”). As this report went to print, the FCC proposed a number of changes to how the Robocall Mitigation Database (RMD) would operate, including removing a provider from the RMD based on affiliations with a known bad actor, and revoking a provider’s international operating authority for repeat offenses. See Sixth Report and Order at ¶ 207, *supra* note 117.
181. The ITG currently considers a compliant response to be one provided within four business days (or within eight business days if the provider is new). Industry Traceback Group, presentation at SIPNOC 2022 Webinar Series (Mar. 25, 2022); ITG Policies and Procedures, *supra* note 87. As of May 20, 2022, the FCC requires gateway providers to respond to traceback requests within 24 hours, and proposed extending that requirement to all providers. See *Sixth Report and Order* at ¶¶ 65, 71, 177, *supra* note 117.
182. For example, the FCC might grant a terminating provider a safe harbor if it requires full robocall mitigation by its upstream providers, and requires that the upstream providers also require that of their upstream providers. Alternatively, a safe harbor might be considered if the provider caught and blocked the illegal traffic within a short time after their initial transmission by the provider.
183. Providers may complain that public tracebacks will expose the private agreements between providers to competitors. But this is actually a strength of this proposal, as it will give legitimate providers another incentive to identify scam calls so that those calls do not run through their networks. In addition, even publishing a scaled-back version of every traceback—including just the information regarding the caller, the originating provider, and the gateway provider and the first intermediate provider located in the U.S.—would be immensely helpful to directing resources across entities to combat the robocall scourge.

APPENDIX 1

OTHER INVASIVE ROBOCALLS

Over Four Billion Robocalls Every Month. In the United States, there are more than 1,300 robocalls answered every second.¹ (See Appendix 2 for a breakdown of the number of robocalls by state.) Indeed, the number of robocalls per year has grown in the past five years. As Table A1-1 illustrates, the number of robocalls increased from a low of 30 billion in 2017 to over 50 billion in 2021.

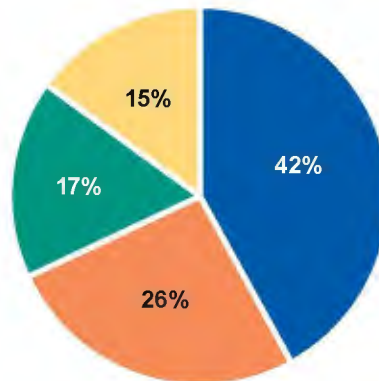


1. There were 1.6 thousand robocalls placed every second in February 2022 (YouMail, [February 2022 Nationwide Robocall Data](#); 1.5 thousand every second in January 2022 (YouMail, [January 2022 Nationwide Robocall Data](#); 1.3 thousand every second in December 2021 (YouMail, [December 2021 Nationwide Robocall Data](#), and 1.6 thousand every second in November 2021 (YouMail, [November 2021 Nationwide Robocall Data](#)).

2. YouMail estimates that there were 30.5 billion robocalls placed in 2017, 47.8 billion calls placed in 2018, 58.5 billion placed in 2019, 45.8 billion placed in 2020, and 50.5 billion placed in 2021. YouMail, [Historical Robocalls By Time](#).

TABLE A1-2

Breakdown of Types of Robocalls in 2021³



■ Scams ■ Alerts and reminders ■ Telemarketing ■ Payment reminders

Wanted Robocalls. Many robocalls are perfectly legal—indeed many robocalls are appreciated by recipients, particularly the 26% of robocalls that are alerts and reminders.⁴ These desired calls include:

- Calls regarding emergencies
- Medical appointment reminders
- Prescription drug reminders
- Financial institution alerts about low balances, potential frauds, or scheduled payments
- Airline updates

Robocalls about emergencies are always legal.⁵ And many non-emergency alerts and reminders provided by either robocall or automated texts have been consented to by the recipients, so are legal. In addition, some informational alerts, including certain messages sent by financial institutions and health services providers, are permitted without consent by exemptions provided by the FCC.⁶

3. PR Newswire, [Americans Hit by Just Under 46 Billion Robocalls in 2020, Says YouMail Robocall Index](#) (Jan. 26, 2021).

4. *See id.*

5. 47 U.S.C. § 227(b); 47 C.F.R. § 64.1200(a)(3)(i).

6. 47 C.F.R. § 64.1200(a)(9)(iii) (financial institution calls), (a)(9)(iv) (health care provider calls).

Debt Collection Robocalls. Another 15% of robocalls are calls made by creditors or debt collectors attempting to collect debts—meaning that over 560 million robocalls are made each month to collect debts. Indeed, nine of the top fifteen robocallers in March 2022 made debt collection calls.⁷

If the collection calls are robocalls sent to cell phones, these calls are legal only if they are made to recipients who have provided consent for the calls.⁸ (Debt collection robocalls to landlines are currently legal without consent, but a pending FCC regulation will limit debt collection robocalls to residential lines to three per month once it goes into effect.⁹) Most courts have held that a consumer who has given a creditor consent to be contacted by a robocall can revoke that consent at any time.¹⁰ The high number of cases filed regarding these debt collection calls in the past few years indicates that many of these debt collection robocalls are made without consent, or after consent has been withdrawn.¹¹

Telemarketing Robocalls. Nearly one fifth of all robocalls¹²—approximately 1 billion—made each month are telemarketing robocalls, which are illegal to cell phones and to residential landlines unless the recipient has provided prior express *written* consent.¹³ Unwanted telemarketing calls are annoying and invasive. In this report we distinguish between telemarketing calls and scam calls because telemarketers are selling real products—although this is not a bright line, as many telemarketing calls sell products that are worthless.

Charitable, Political, Informational and Survey Robocalls. Unless an emergency is involved, prerecorded calls to cell phones are legal only with the prior consent of the called party—and as this rule applies regardless of the content of the call, it applies to charitable, political, survey, and informational calls.¹⁴ The FCC has announced limits to these prerecorded calls to residential landlines, but implementation has been delayed.¹⁵

7. See YouMail, [Top 100 Volume Robocallers Nationwide in March 2022](#) (last visited on Apr. 5, 2022).

8. 47 U.S.C. § 227(b)(1)(A).

9. See *In re* Rules and Regulations Implementing the Tel. Consumer Prot. Act of 1991, [Report and Order, CG Docket No. 02-278, FCC 20-186](#) (Dec. 30, 2020) [hereinafter TRACED Act Section 8 Report and Order].

10. See National Consumer Law Center, *Federal Deception Law* § 6.3.6.5.3 (4th ed. 2022).

11. See *id.* at § 6.3.6.5.

12. PR Newswire, *50 Billion Robocalls in 2021*, *supra* note 4.

13. See 47 C.F.R. § 64.1200(a)(2). Additionally, live telemarketing calls are illegal when made to a residential line (whether landline or cell phone) that has been registered on the Do Not Call Registry, unless the recipient has provided prior express written consent. 47 C.F.R. § 64.1200(c)(2)(ii).

14. See 42 U.S.C. § 227(b)(1).

15. See TRACED Act Section 8 Report and Order, *supra* note 9.

Robot Calls. Many people believe that when they receive a call that begins with “May I speak with ‘caller’s name’. . . .” the call is not a robocall because the recipient’s name is included and there appears to be some conversation with the caller. However, many of these personalized calls are indeed robocalls, as robocalls often are keyed to information provided from the dark web, and modern robocalling equipment now includes “soundboard technology” that allows a human operator to manipulate the prerecorded clips.¹⁶ As soundboard calls use prerecorded voices they are considered robocalls that are covered by the consent requirements for prerecorded calls.¹⁷ Indeed, according to YouMail, soundboard technology has been increasingly used in robocalls, including scam robocalls, in the past three years, beginning with fewer than 50,000 per month in early 2019 and rising to around 450,000 per month in March 2022, an increase of more than 750% in three years.¹⁸

16. Calls using soundboard technology such as Yodel’s are often referred to as “robot calls.” See Lexology, [Robot Calling? Better Have Consent](#).

17. See *Braver v. NorthStar Alarm Servs., L.L.C.*, 2019 WL 3208651, at *5–6 (W.D. Okla. July 16, 2019). (“The soundboard software (referred to by Yodel as ‘the Yodel Dialer’) required Yodel’s soundboard agents, located in a call center in India, to follow a script which instructed them to press buttons in a certain order thereby delivering prerecorded audio clips to the called party.”), reconsideration denied, 2019 WL 5722207 (W.D. Okla. Nov. 5, 2019). Also see [Staff Opinion Letter from Lois Greisman, Associate Director, Division of Marketing Practices, Federal Trade Commission, to Michael Bills, CEO, Call Assistant, L.L.C.](#) (Nov. 10, 2016), (“[O]utbound telemarketing calls that utilize soundboard technology are subject to the TSR’s prerecorded call provisions because *such calls do, in fact, ‘deliver a prerecorded message’* as set forth in the plain language of the [Telemarketing Sales Rule.]”) (emphasis added).

18. Email from Mike Rudolph, YouMail Chief Technology Officer, to Margot Saunders (Apr. 1, 2022).

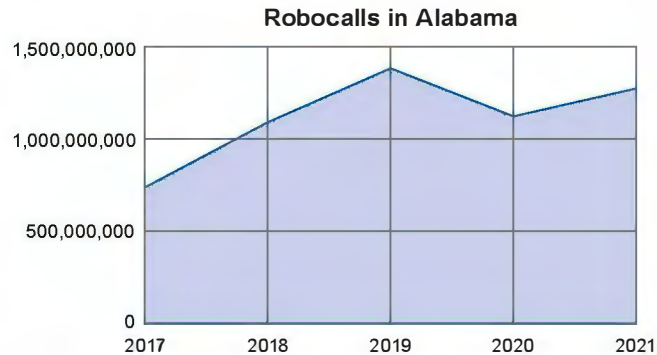
APPENDIX 2

SCAM ROBOCALLS IN THE STATES

Scam Robocalls in Alabama

News reports reveal that scammers are sending robocalls to telephone subscribers in Alabama and falsely threatening to cut off their electric power because of “unpaid bills” unless the consumers make immediate payments over the phone.¹

Scams like this one make up some of the 5.3 million scam “electric bill” robocalls that deluged consumers in Alabama and across the nation in January 2022 alone.²



Scam electric bill calls only make up part of the scam robocall problem. **In 2021, Alabama residents received nearly 1.3 billion robocalls** (see Robocalls in Alabama graph), **about 533 million (42%) of which were scam robocalls.** This meant that approximately 11 scam robocalls were made to every Alabama resident per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, more than half a million Alabama residents lost money to scam robocalls in 2021.⁵

1. Alabama NewsCenter, “[Phone scammers at it again in Alabama](#)” (Sept. 14, 2021).

2. YouMail confidential data provided to NCLC, filtered by campaigns related to electric bill scams.

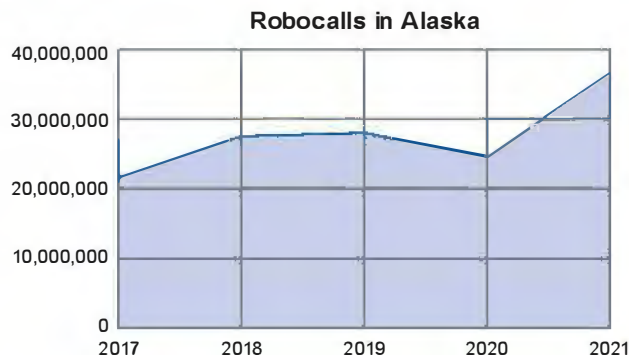
3. YouMail, “[Historical Robocalls by State](#)” (2022). YouMail, “[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#),” PR NewsWire (Jan. 6, 2022). Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Alabama and then calculated the number per adult Alabaman (see note 5) per month.

4. Roger Grimes, “[Smishing 101 and Defenses](#),” KnowBe4 (Jan. 8, 2020).

5. TrueCaller, “[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)” (2021). Truecaller’s survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Alabama’s adult population (3,921,024 in 2021, per the [U.S. Census Bureau](#)) is 541,101.

Scam Robocalls in Alaska

News reports reveal that Alaskans are being targeted by a telephone scam in which scammers, pretending to be from the U.S. Marshals, threaten their victims with arrest unless they hand over their personal and banking information.¹ Scams like this one make up some of the 4.3 million scam “arrest warrant” robocalls that deluged consumers nationwide in January 2022.²



Fake arrest warrants only make up part of the problem. According to estimates based on data from YouMail, the most prevalent scam campaigns of January 2022 accounted for nearly 1 million scam robocalls made to Alaska phones in that month alone, and these top campaigns are only a portion of the total scam robocalls made.³ **In 2021, Alaskans received more than 38 million robocalls (see Robocalls in Alaska graph), about 15.6 million (42%) of which were scam robocalls**—or between 2 and 3 scam robocalls for each Alaskan per month.⁴ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁵

These robocalls have a cost. According to estimates based on TrueCaller survey data, more than 76,000 Alaskans lost money to scam robocalls in 2021.⁶

1. Matt Miller, “[Don’t answer the call’: federal agency warns of phone scam sweeping Alaska](#),” KTOO (April 28, 2021).

2. YouMail confidential data provided to NCLC, filtered by campaigns related to arrest warrant scams.

3. Id., all campaigns. We multiplied the number of calls from the top 1,000 scam robocall campaigns nationwide in January by Alaska’s share of the US adult population (0.2%) to estimate calls to Alaska phones in January.

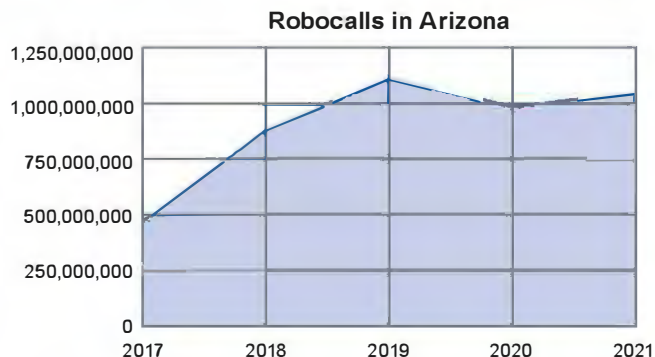
4. YouMail, “[Historical Robocalls by State](#)” (2022). Id., “[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#),” PR NewsWire (Jan. 6, 2022). Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Alaska and then calculated the number per adult Alaskan (see note 6) per month.

5. Roger Grimes, “[Smishing 101 and Defenses](#),” KnowBe4 (Jan. 8, 2020).

6. TrueCaller, “[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)” (2021). Truecaller’s survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Alaska’s adult population (552,435 in 2021, per the [U.S. Census Bureau](#)) is 76,236.

Scam Robocalls in Arizona

Arizona’s Attorney General warned residents last year of a common robocall scam. The scammer pretends to be calling from a retail company, warns the victim of an “unauthorized purchase,” and then attempts to gain the victim’s bank or credit card information.¹



This kind of scam is far from rare.

According to estimates based on data from YouMail, more than 300,000 scam “fraud alert” robocalls were made to Arizona phones in January 2022 alone.² **In 2021, Arizona received about 1 billion robocalls** (see Robocalls in Arizona graph), **about 444 million (42%) of which were scam robocalls**—or between 6 and 7 scam robocalls for each Arizonan per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, almost 780,000 Arizonans lost money to scam robocalls in 2021.⁵

1. Fox 10 Phoenix, “[Arizona Attorney General warns of ‘unauthorized purchase’ phone scams](#)” (Sept. 11, 2021).

2. YouMail confidential data provided to NCLC, filtered by campaigns related to fraud alerts. We multiplied nationwide scam fraud alert robocalls made in January by Arizona’s share of the US adult population (2.2%) to estimate calls made to Arizona phones in January.

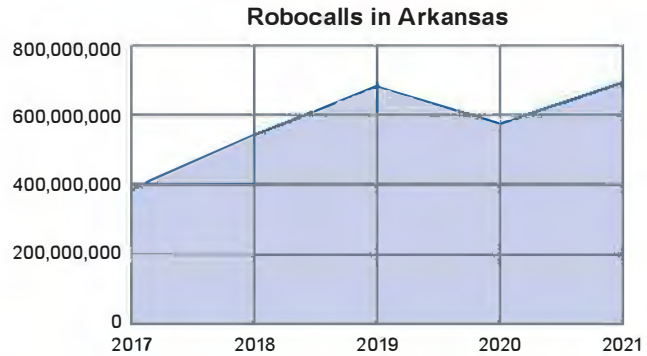
3. YouMail, “[Historical Robocalls by State](#)” (2022). YouMail, “[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#),” PR NewsWire (Jan. 6, 2022). Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Arizona and then calculated the number per adult Arizonan (see note 5) per month.

4. Roger Grimes, “[Smishing 101 and Defenses](#),” KnowBe4 (Jan. 8, 2020).

5. TrueCaller, “[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)” (2021). Truecaller’s survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Arizona’s adult population (5,639,145 in 2021, per the [U.S. Census Bureau](#)) is 778,202.

Scam Robocalls in Arkansas

Arkansas' Attorney General reported an increase in Social Security-related robocalls scams. Scammers claiming to be from the Social Security Administration have targeted Arkansas consumers, threatening them into making payments or providing personal information.¹



This kind of scam is not rare.

According to estimates based on data from YouMail, nearly 80,000 scam Social Security robocalls were made to Arkansas phones in January 2022 alone.² **In 2021, Arkansans received nearly 700 million robocalls (see Robocalls in Arkansas graph), almost 300 million (42%) of which were scam robocalls—or between 10 and 11 scam robocalls for each Arkansan per month.**³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, more than 320,000 Arkansans lost money to scam robocalls in 2021.⁵

1. Ozark Radio News, "[Scams targeting Arkansans' social security numbers](#)" (July 23, 2020).

2. YouMail confidential data provided to NCLC, filtered by campaigns related to Social Security scams. We multiplied nationwide scam Social Security robocalls in January by Arkansas' share of the US adult population (0.9%) to estimate calls made to Arkansas phones in January.

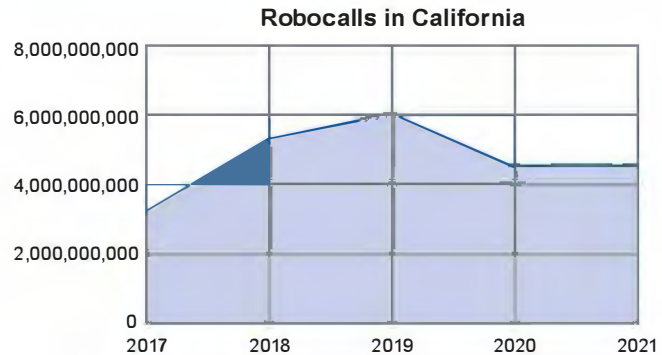
3. YouMail, "[Historical Robocalls by State](#)" (2022). YouMail, "[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#)," PR NewsWire (Jan. 6, 2022). Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Arkansas and then calculated the number per adult Arkansan (see note 5) per month.

4. Roger Grimes, "[Smishing 101 and Defenses](#)," KnowBe4 (Jan. 8, 2020).

5. TrueCaller, "[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)" (2021). Truecaller's survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Arkansas' adult population (2,323,884 in 2021, per the [U.S. Census Bureau](#)) is 320,696.

Scam Robocalls in California

One California consumer received a robocall that purported to be from Norton Antivirus, telling him he was entitled to a \$400 refund. When he called back, a scammer convinced him to grant remote access to his computer to process the transaction, but then suddenly insisted he had accidentally been overpaid. The consumer did see an “overpayment” in his account—but what he did not realize was that it was his own money, which the scammers had secretly transferred there from another of his accounts after gaining access to his computer. The scammer convinced him to send the money back using a \$4,000 Google gift card. Only days later, the call center contacted the consumer again, telling him that the “agent” he had previously spoken to had been fired for fraud and that he was owed a refund on the \$4,000 he had sent. The consumer was convinced to repeat the whole scam again, this time losing \$14,000.¹



Sadly, this consumer is far from the only Californian to encounter this kind of robocall scam. According to estimates based on data from YouMail, more than 34,000 scam robocalls touting fake refunds were made to California phones in January 2022 alone.² **In 2021, Californians received more than 4.5 billion robocalls** (see Robocalls in California graph), **nearly 2 billion (42%) of which were scam robocalls**—or between 5 and 6 scam robocalls for each Californian per month.³ And fraudulent calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, more than 4 million Californians lost money to scam robocalls in 2021.⁵

1. Jeremy Roebuck, “Americans lost \$150M to robocall scams last year. Students from India came to PA and NJ to collect, feds say,” Philadelphia Inquirer (Aug. 11, 2020).

2. YouMail confidential data provided to NCLC, filtered by campaigns related to refunds. We multiplied nationwide scam refund robocalls in January by California’s share of the US adult population (11.8%) to estimate calls made to California phones in January.

3. YouMail, “Historical Robocalls by State” (2022). YouMail, “U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index,” PR NewsWire (Jan. 6, 2022). Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in California and then calculated the number per adult Californian (see note 5) per month.

4. Roger Grimes, “Smishing 101 and Defenses,” KnowBe4 (Jan. 8, 2020).

5. TrueCaller, “TrueCaller Insights 2021 U.S. Spam & Scam Report” (2021). Truecaller’s survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of California’s adult population (30,409,323 in 2021, per the U.S. Census Bureau) is 4,196,487.

Scam Robocalls in Colorado

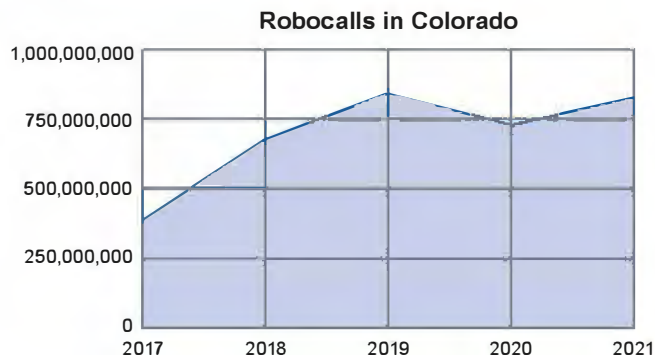
Colorado ranks third in the nation for robocalls per person, by some estimates. One of the most prevalent robocall scams in the state is the fake “arrest warrant” scam, in which the scammer claims to be from law enforcement and demands immediate payment from the victim under threat of arrest.

The calls are spoofed so that they appear to be coming from a legitimate law enforcement number.¹

According to estimates based on data from YouMail, nearly 80,000 scam “arrest warrant” robocalls were made to Colorado phones in January 2022 alone.²

In 2021, Coloradans received about 824 million robocalls (see Robocalls in Colorado graph), **346 million (42%) of which were scam robocalls**—or between 6 and 7 scam robocalls for each Coloradans per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, well over half a million Coloradans lost money to scam robocalls in 2021.⁵



1. Randy Wyrick, “[Sick of getting robocalls? Colorado ranks third in number of robocalls per person](#),” Vail Daily (Jan. 6, 2020). Per this VailDaily article, Colorado’s “third” ranking is based on FTC complaints as well as YouMail data.

2. YouMail confidential data provided to NCLC. We multiplied the number of calls from the top 1,000 scam robocall campaigns nationwide in January by Colorado’s share of the US adult population (1.8%) to estimate calls made to Colorado phones in January.

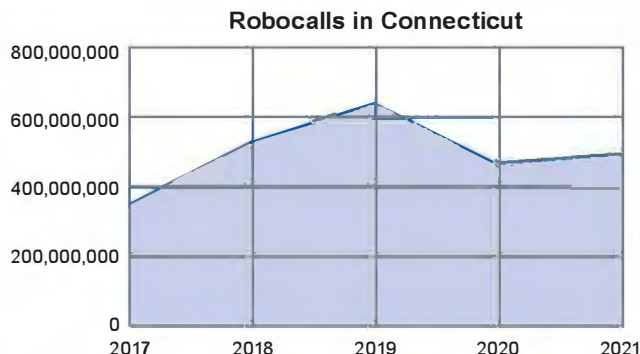
3. YouMail, “[Historical Robocalls by State](#)” (2022). YouMail, “[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#),” PR NewsWire (Jan. 6, 2022). Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Colorado and then calculated the number per adult Coloradan (see note 5) per month.

4. Roger Grimes, “[Smishing 101 and Defenses](#),” KnowBe4 (Jan. 8, 2020).

5. TrueCaller, “[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)” (2021). Truecaller’s survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Colorado’s adult population (4,539,226 in 2021, per the [U.S. Census Bureau](#)) is 626,413.

Scam Robocalls in Connecticut

Last year, Connecticut’s Attorney General helped to shut down a nationwide scam “charitable fundraising” organization that made over a billion robocalls and stole \$110 million from consumers. More than 34 million of those robocalls were made to Connecticut consumers, including to some families who received multiple robocalls per hour.¹



Although this particular scam operation has been shut down, the problem of fraudulent robocalls continues. According to estimates based on data from YouMail, the most prevalent scam campaigns of January 2022 accounted for more than 5 million scam robocalls made to Connecticut phones in that month alone, and these top campaigns are only a portion of the total scam robocalls made.² **In 2021, Connecticut residents received nearly 500 million robocalls (see Robocalls in Connecticut graph), about 200 million (42%) of which were scam robocalls**—or between 5 and 6 scam robocalls for each Connecticut resident per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, nearly 400,000 Connecticut residents lost money to scam robocalls in 2021.⁵

1. Zach Murdock, “Connecticut joins settlement to shut down massive robocall fundraising scam that made more than 1 billion calls,” Hartford Courant (March 4, 2021)

2. YouMail confidential data provided to NCLC. We multiplied the number of calls from the top 1,000 scam robocall campaigns nationwide in January by Connecticut’s share of the US adult population (1.1%) to estimate calls made to Connecticut phones in January.

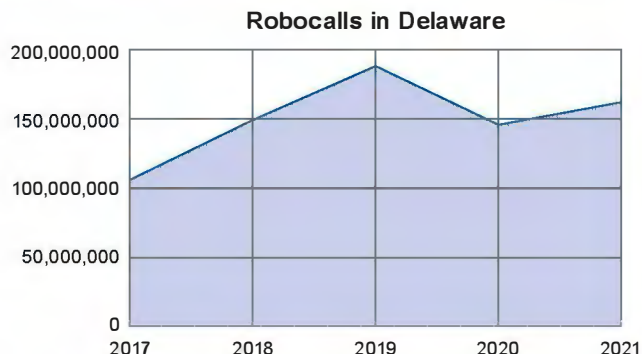
3. YouMail, “Historical Robocalls by State” (2022). YouMail, “U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index,” PR NewsWire (Jan. 6, 2022). Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Connecticut and then calculated the number per adult Connecticut resident (see note 5) per month.

4. Roger Grimes, “Smishing 101 and Defenses,” KnowBe4 (Jan. 8, 2020).

5. TrueCaller, “TrueCaller Insights 2021 U.S. Spam & Scam Report” (2021). Truecaller’s survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Connecticut’s adult population (2,870,055 in 2021, per the U.S. Census Bureau) is 396,068.

Scam Robocalls in Delaware

Last year the Delaware State Police warned residents of scam robocalls making the rounds. In these calls scammers claimed to be from the police and demanded that victims make immediate payments to avoid criminal charges. The scammers' phone numbers had been spoofed to appear as the Delaware State Police's real number.¹



This is a common scam. According to estimates based on data from YouMail, more than 13,000 scam “arrest warrant” robocalls were made to Delaware phones in January 2022 alone.² **In 2021, Delawareans received more than 160 million robocalls** (see Robocalls in Delaware graph), **about 68 million (42%) of which were scam robocalls**—or about 7 scam robocalls for each Delawarean per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, more than 100,000 Delawareans lost money to scam robocalls in 2021.⁵

1. Betsy Price, “[Delaware State Police: Scammer is using number that appears to belong to them](#),” Delaware Live (Jan. 20, 2021).

2. YouMail confidential data provided to NCLC, filtered by campaigns related to arrest warrants. We multiplied nationwide scam arrest warrant robocalls in January by Delaware’s share of the US adult population (0.3%) to estimate calls made to Delaware phones in January.

3. YouMail, “[Historical Robocalls by State](#)” (2022). YouMail, “[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#),” PR NewsWire (Jan. 6, 2022). Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Delaware and then calculated the number per adult Delawarean (see note 5) per month.

4. Roger Grimes, “[Smishing 101 and Defenses](#),” KnowBe4 (Jan. 8, 2020).

5. TrueCaller, “[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)” (2021). Truecaller’s survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Delaware’s adult population (793,677 in 2021, per the [U.S. Census Bureau](#)) is 109,527.

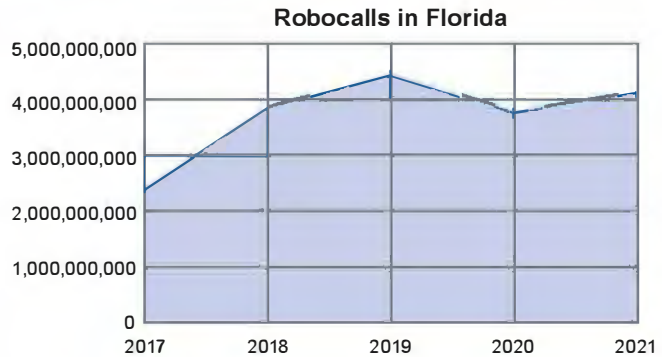
Scam Robocalls in Florida

“Ann,” a Florida woman, received a robocall saying that her Social Security number had been compromised and she needed to speak to an investigator. When she dialed back, she was told that she was under investigation by federal authorities for money laundering and drug charges, that her Social Security number and bank accounts would be

suspended, and that she needed to get as much cash as possible out of the accounts first. The scammer told her that she was under surveillance and needed to stay on the line with him on speaker at every bank she visited. Ann went to a bank and withdrew \$2,500, then followed the scammer’s instructions to buy five Target gift cards and four CVS gift cards, totaling thousands of dollars. She read the gift card numbers to him over the phone. The scammer kept her on the phone for over 5 hours, and by the time she got home her husband had called the police, thinking she had been kidnapped. By the time police told Ann that this was a scam, she had already lost all the money she spent on the gift cards.¹

Sadly, Ann is far from the only Floridian to encounter this kind of robocall scam. According to estimates based on data from YouMail, more than 587,000 scam Social Security robocalls were made to Florida phones in January 2022 alone.² **In 2021, Floridians received more than 4.1 billion robocalls** (see Robocalls in Florida graph), **about 1.7 billion (42%) of which were scam robocalls**—or more than 8 scam robocalls for each Floridian per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, nearly two and half million Floridians lost money to scam robocalls in 2021.⁵



1. “Gift Card Scam,” Florida Office of the Attorney General (filed April 22, 2021), received via email from Patrick Crotty on March 2, 2022.

2. YouMail confidential data provided to NCLC, filtered by campaigns related to Social Security scams. We multiplied nationwide scam Social Security robocalls in January by Florida’s share of the US adult population (6.8%) to estimate calls made to Florida phones in January.

3. YouMail, “[Historical Robocalls by State](#)” (2022). YouMail, “[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#),” PR NewsWire (Jan. 6, 2022). Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Florida and then divided per adult Floridian (see note 5) per month.

4. Roger Grimes, “[Smishing 101 and Defenses](#),” KnowBe4 (Jan. 8, 2020).

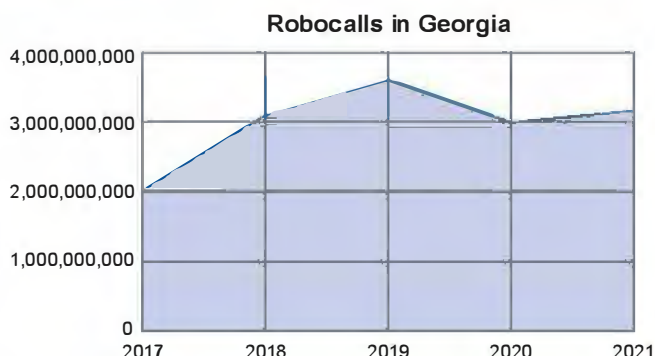
5. TrueCaller, “[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)” (2021). Truecaller’s survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Florida’s adult population (17,490,246 in 2021, per the [U.S. Census Bureau](#)) is 2,413,654.

Scam Robocalls in Georgia

Georgia’s Attorney General warned residents last year of a robocall scam claiming to be from the AG’s own office. The robocall told victims it was regarding “your case” and urged them to respond to avoid consequences.¹

But this is not the only robocall scam targeting Georgians.

According to estimates based on data from YouMail, the most prevalent scam campaigns of January 2022 accounted for more than 14.6 million scam robocalls made to Georgia phones in that month alone, and these top campaigns are only a portion of the total scam robocalls made.² **In 2021, Georgians received more than 3 billion robocalls** (see Robocalls in Georgia graph), **about 1.3 billion (42%) of which were scam robocalls**—or about 13 scam robocalls for each Georgian per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴



These robocalls have a cost. According to estimates based on TrueCaller survey data, more than a million Georgians lost money to scam robocalls in 2021.⁵

1. Georgia Attorney General's Office, "[Scam Alert: Carr warns of fake calls from scammers posing as Attorney General's office](#)" (May 3, 2021).

2. YouMail confidential data provided to NCLC. We multiplied the number of calls from the top 1,000 scam robocall campaigns nationwide in January by Georgia's share of the US adult population (3.2%) to estimate calls made to Georgia phones in January.

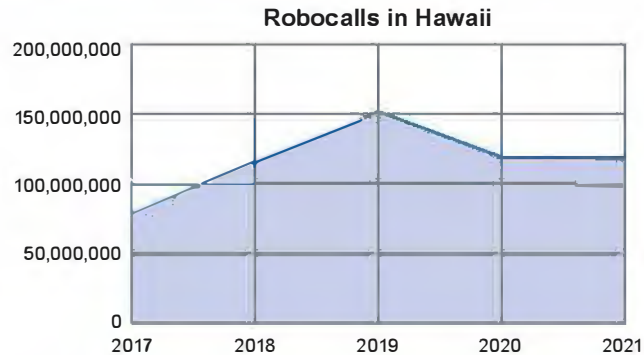
3. YouMail, "[Historical Robocalls by State](#)" (2022). YouMail, "[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#)," PR NewsWire (Jan. 6, 2022). Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Georgia and then calculated the number per adult Georgian (see note 5) per month.

4. Roger Grimes, "[Smishing 101 and Defenses](#)," KnowBe4 (Jan. 8, 2020).

5. TrueCaller, "[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)" (2021). Truecaller's survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Georgia's adult population (8,250,868 in 2021, per the [U.S. Census Bureau](#)) is 1,138,620.

Scam Robocalls in Hawaii

Hawaii's state Sheriff Division warned residents earlier this year about a robocall scam making the rounds. Scammers pretending to be from the sheriff's office told victims that there was a warrant out for their arrest, and they needed to make payments to avoid arrest.¹



This kind of scam is far from rare.

According to estimates based on data from YouMail, more than 17,000 scam “arrest warrant” robocalls were made to Hawaii phones in January 2022 alone.²

In 2021, Hawaiians received nearly 120 million robocalls (see Robocalls in Hawaii graph), almost 50 million (42%) of which were scam robocalls—or between 3 and 4 scam robocalls for each Hawaiian per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, more than 150,000 Hawaiians lost money to scam robocalls in 2021.⁵

1. Scott Kim, “[Beware of an arrest warrant phone call scam, state Sheriff Division says](#),” Hawaii Public Radio (Jan. 25, 2022).

2. YouMail confidential data provided to NCLC, filtered by campaigns related to arrest warrants. We multiplied nationwide scam arrest warrant robocalls in January by Hawaii's share of the US adult population (0.4%) to estimate calls made to Hawaii phones in January.

3. YouMail, “[Historical Robocalls by State](#)” (2022). YouMail, “[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#).” Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Hawaii and then calculated the number per adult Hawaiian (see note 5) per month.

4. Roger Grimes, “[Smishing 101 and Defenses](#),” KnowBe4 (Jan. 8, 2020).

5. TrueCaller, “[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)” (2021). Truecaller's survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Hawaii's adult population (1,135,944 in 2021, per the [U.S. Census Bureau](#)) is 156,760.

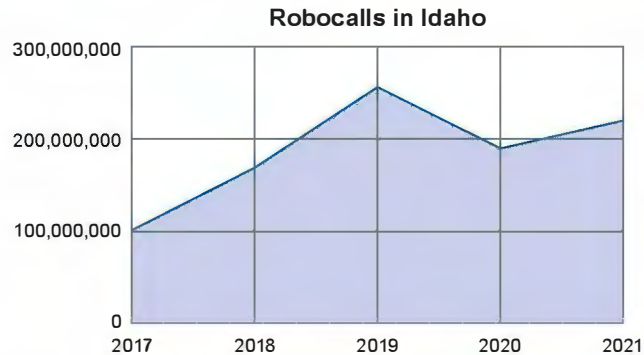
Scam Robocalls in Idaho

Robocall scammers claiming to be from the Social Security Administration have targeted Idaho consumers. These scammers have threatened Idahoans into making payments or providing personal information.¹

This kind of scam is not rare.

According to estimates based on data from YouMail, more than 51,000 scam Social Security robocalls were made to Idaho phones in January 2022 alone.² **In 2021, Idahoans received more than 220 million robocalls** (see Robocalls in Idaho graph), **more than 93 million (42%) of which were scam robocalls**—or between 5 and 6 scam robocalls for each Idahoan per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, nearly 200,000 Idahoans lost money to scam robocalls in 2021.⁵



1. Alejandra Buitrago, "[Social Security scam targets Idaho residents](#)", Idaho Mountain Express (Aug. 23, 2019).

2. YouMail confidential data provided to NCLC, filtered by campaigns related to Social Security scams. We multiplied nationwide scam Society Security robocalls in January by Idaho's share of the US adult population (0.6%) to estimate calls made to Idaho phones in January.

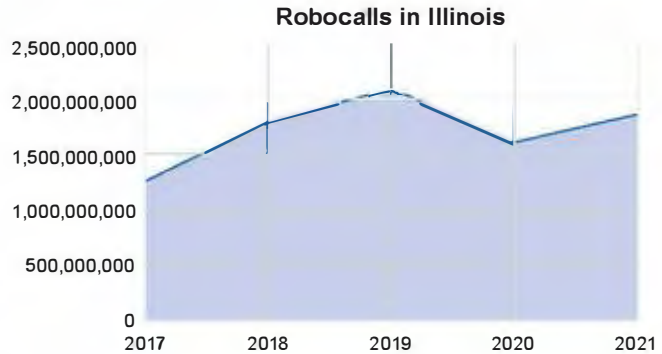
3. YouMail, "[Historical Robocalls by State](#)" (2022). YouMail, "[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#)." Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Idaho and then divided per adult Idahoan (see note 5) per month.

4. Roger Grimes, "[Smishing 101 and Defenses](#)," KnowBe4 (Jan. 8, 2020).

5. TrueCaller, "[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)" (2021). Truecaller's survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Idaho's adult population (1,423,791 in 2021, per the [U.S. Census Bureau](#)) is 196,483.

Scam Robocalls in Illinois

Scammers in Illinois have used the COVID-19 pandemic as a springboard for fraud. They have placed thousands of calls to Illinois consumers, posing as government employees offering to “help” with driver’s licenses and unemployment benefits.¹



But these are not the only robocall scams targeting

Illinoisans. According to estimates based on data from YouMail, the most prevalent scam campaigns of January 2022 accounted for more than 17.4 million scam robocalls made to Illinois phones in that month alone, and these top campaigns are only a portion of the total scam robocalls made.² **In 2021, Illinoisans received nearly 2 billion robocalls** (see Robocalls in Illinois graph), **nearly 800 million (42%) of which were scam robocalls**—or between 6 and 7 scam robocalls for each Illinoisan per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, more than 1.3 million Illinoisans lost money to scam robocalls in 2021.⁵

1. Better Business Bureau, “[Scammers continue to target Illinoisans, BBB warns](#),” NBC 5 Chicago (July 27, 2021).

2. YouMail confidential data provided to NCLC. We multiplied the number of calls from the top 1,000 scam robocall campaigns nationwide in January by Illinois’ share of the US adult population (3.8%) to estimate calls made to Illinois phones in January.

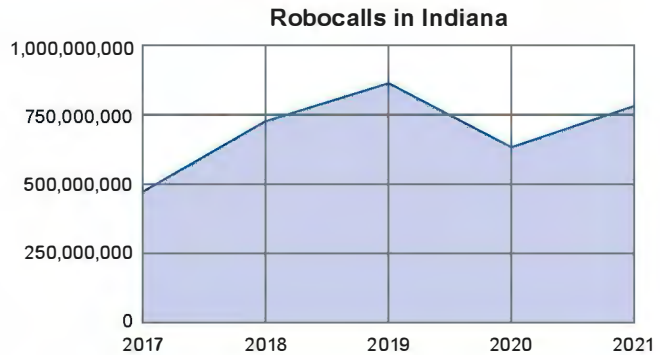
3. YouMail, “[Historical Robocalls by State](#)” (2022). YouMail, “[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#).” Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Illinois and then calculated the number per adult Illinoisan (see note 5) per month.

4. Roger Grimes, “[Smishing 101 and Defenses](#),” KnowBe4 (Jan. 8, 2020).

5. TrueCaller, “[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)” (2021). Truecaller’s survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Illinois’ adult population (9,858,403 in 2021, per the [U.S. Census Bureau](#)) is 1,360,460.

Scam Robocalls in Indiana

Indiana’s Attorney General last year warned of a marked increase in scam robocalls targeting residents, after a slight slump during the first year of the pandemic. One couple reported receiving ten calls in just a few hours, including some from scammers spoofing phone numbers that had belonged to deceased friends.¹



But these are not the only robocall scams targeting Hoosiers. According to estimates based on data from YouMail, the most prevalent scam campaigns of January 2022 accounted for more than 9.1 million scam robocalls made to Indiana phones in that month alone, and these top campaigns are only a portion of the total scam robocalls made.² **In 2021, Hoosiers received more than 780 million robocalls** (see Robocalls in Indiana graph), **nearly 330 million (42%) of which were scam robocalls**—or about 5 scam robocalls for each Hoosier per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, more than 720,000 Hoosiers lost money to scam robocalls in 2021.⁵

1. Carly Miller, “Robocalls increasing, what to do about them,” 16 News Now (June 18, 2021).

2. YouMail confidential data provided to NCLC. We multiplied the number of calls from the top 1,000 scam robocall campaigns nationwide in January by Indiana’s share of the US adult population (2%) to estimate calls made to Indiana phones in January.

3. YouMail, “Historical Robocalls by State” (2022). YouMail, “U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index.” Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Indiana and then calculated the number per adult Hoosier (see note 5) per month.

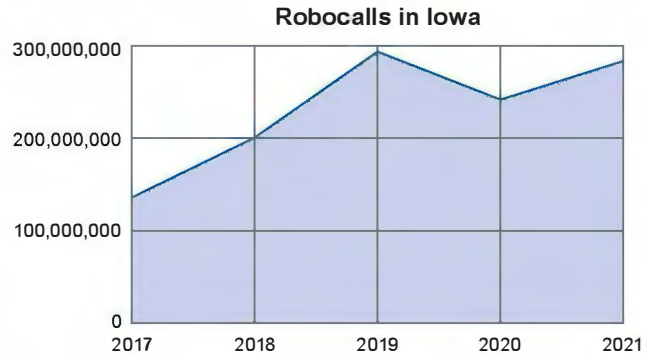
4. Roger Grimes, “Smishing 101 and Defenses,” KnowBe4 (Jan. 8, 2020).

5. TrueCaller, “TrueCaller Insights 2021 U.S. Spam & Scam Report” (2021). Truecaller’s survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Indiana’s adult population (5,220,190 in 2021, per the U.S. Census Bureau) is 720,386.

Scam Robocalls in Iowa

Iowa's Attorney General warned fed-up residents last year not to answer calls from unknown numbers. This was due to the rise in scam robocalls targeting Iowans.¹

According to estimates based on data from YouMail, the most prevalent scam campaigns of January 2022 accounted for more than 4.5 million scam robocalls made to Iowa phones in that month alone, and these top campaigns are only a portion of the total scam robocalls made.² **In 2021, Iowans received more than 280 million robocalls (see Robocalls in Iowa graph), nearly 120 million (42%) of which were scam robocalls**—or about 4 scam robocalls for each Iowan per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴



These robocalls have a cost. According to estimates based on TrueCaller survey data, well over a quarter million Iowans lost money to scam robocalls in 2021.⁵

1. Rachel Droze, “‘Don’t answer’: Iowa’s AG office says ignore numbers you don’t know if possible to fight robocalls,” WeAreIowa.com (May 13, 2021).

2. YouMail confidential data provided to NCLC. We multiplied the number of calls from the top 1,000 scam robocall campaigns nationwide in January by Iowa’s share of the US adult population (1%) to estimate calls made to Iowa phones in January.

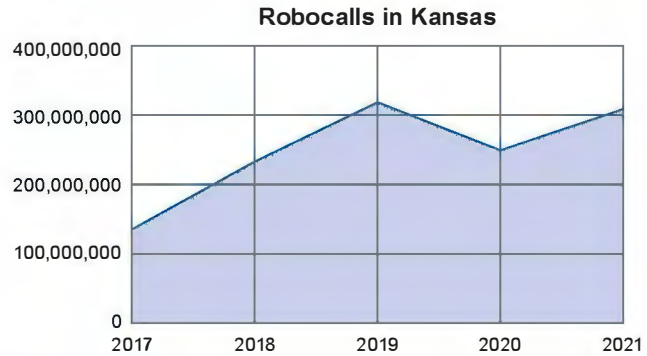
3. YouMail, “Historical Robocalls by State” (2022). YouMail, “U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index.” Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Iowa and then divided per adult Iowan (see note 5) per month.

4. Roger Grimes, “Smishing 101 and Defenses,” KnowBe4 (Jan. 8, 2020).

5. TrueCaller, “TrueCaller Insights 2021 U.S. Spam & Scam Report” (2021). Truecaller’s survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Iowa’s adult population (2,458,671 in 2021, per the U.S. Census Bureau) is 339,297.

Scam Robocalls in Kansas

Kansas' Attorney General warned residents this tax season to beware of scam "IRS" robocalls. Scammers claim that a victim owes taxes and threaten the victim into paying immediately over the phone, often in the form of gift cards.¹



But these are not the only robocall scams targeting

Kansans. According to estimates based on data from YouMail, the most prevalent scam campaigns of January 2022 accounted for more than 4.1 million scam robocalls made to Kansas phones in that month alone, and these top campaigns are only a portion of the total scam robocalls made.² **In 2021, Kansans received more than 300 million robocalls** (see Robocalls in Kansas graph), **nearly 130 million (42%) of which were scam robocalls**—or between 4 and 5 scam robocalls for each Kansan per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, well over a quarter million Kansans lost money to scam robocalls in 2021.⁵

1. Kansas Attorney General's Office, "[AG Derek Schmidt urges Kansans to be wary of scams during tax season](#)" (March 28, 2022).

2. YouMail confidential data provided to NCLC. We multiplied the number of calls from the top 1,000 scam robocall campaigns nationwide in January by Kansas' share of the US adult population (0.9%) to estimate calls made to Kansas phones in January.

3. YouMail, "[Historical Robocalls by State](#)" (2022). YouMail, "[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#)." Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Kansas and then calculated the number per adult Kansan (see note 5) per month.

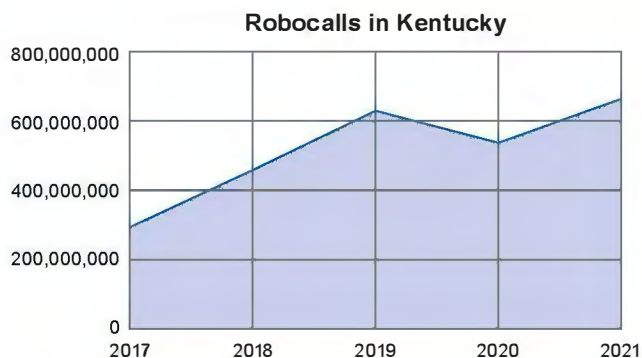
4. Roger Grimes, "[Smishing 101 and Defenses](#)," KnowBe4 (Jan. 8, 2020).

5. TrueCaller, "[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)" (2021). Truecaller's survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Kansas' adult population (2,230,282 in 2021, per the [U.S. Census Bureau](#)) is 307,779.

Scam Robocalls in Kentucky

Robocall scammers claiming to be from the Social Security Administration have targeted Kentucky consumers. These scammers threaten Kentuckians into making payments or providing personal information.¹

This kind of scam is not rare. According to estimates based on data from YouMail, more than 120,000 scam Social Security robocalls were made to Kentucky phones in January 2022 alone.² **In 2021, Kentuckians received more than 650 million robocalls** (see Robocalls in Kentucky graph), **nearly 280 million (42%) of which were scam robocalls**—or between 6 and 7 scam robocalls for each Kentuckian per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴



These robocalls have a cost. According to estimates based on TrueCaller survey data, nearly half a million Kentuckians lost money to scam robocalls in 2021.⁵

1. Gilbert Corsey, "[Social Security phone scam sweeping through Louisville](#)," WDRB.com (Jul. 1, 2019, updated Jul. 2, 2019).

2. YouMail confidential data provided to NCLC, filtered by campaigns related to Social Security scams. We multiplied nationwide scam Social Security robocalls in January by Kentucky's share of the US adult population (1.4%) to estimate calls made to Kentucky phones in January.

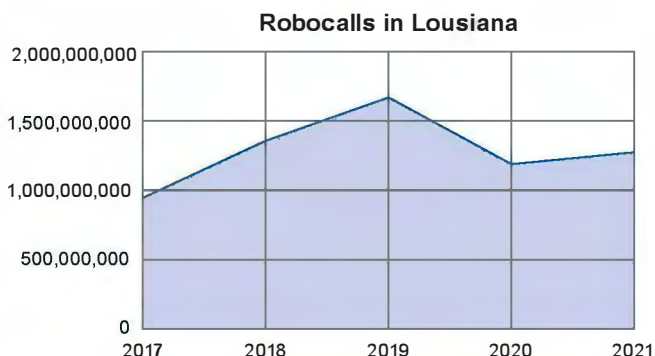
3. YouMail, "[Historical Robocalls by State](#)" (2022). YouMail, "[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#)." Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Kentucky and then calculated the number per adult Kentuckian (see note 5) per month.

4. Roger Grimes, "[Smishing 101 and Defenses](#)," KnowBe4 (Jan. 8, 2020).

5. TrueCaller, "[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)" (2021). Truecaller's survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Kentucky's adult population (3,499,290 in 2021, per the [U.S. Census Bureau](#)) is 482,902. Kentucky consumers reported more than one million dollars in losses from phone scams in 2020. See Steve Rogers, "[AG joins others in asking FCC for faster action on anti-robocall technology](#)," WTVQ/ABC36 (Aug. 9, 2021).

Scam Robocalls in Louisiana

Melinda Walsh of Baton Rouge receives up to eight robocalls per day on her cell phone alone. She has 54 blocked numbers on her phone—but the calls keep coming. Baton Rouge is the robocall capital of the United States; its residents receive as many as 39 robocalls per month.¹ Many of these robocalls are predatory scams designed to take as much money as possible from Louisianans.



According to estimates based on data from YouMail, the most prevalent scam campaigns of January 2022 accounted for more than 6.4 million scam robocalls made to Louisiana phones in that month alone, and these top campaigns are only a portion of the total scam robocalls made.² **In 2021, Louisianans received nearly 1.3 billion robocalls** (see Robocalls in Louisiana graph), **about 535 million (42%) of which were scam robocalls**—or between 12 and 13 scam robocalls for each Louisianan per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, nearly half a million Louisianans lost money to scam robocalls in 2021.⁵

1. Samantha Murphy Kelly, "[What it's like to live in the robocall capital of America](#)," CNN Business (March 16, 2021).

2. YouMail confidential data provided to NCLC. We multiplied the number of calls from the top 1,000 scam robocall campaigns nationwide in January by Louisiana's share of the US adult population (1.4%) to estimate calls made to Louisiana phones in January.

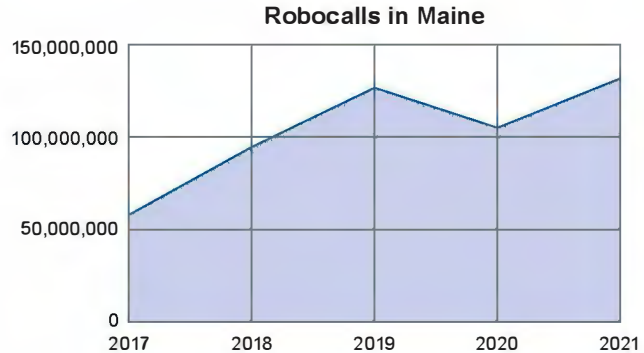
3. YouMail, "[Historical Robocalls by State](#)" (2022). YouMail, "[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#)." Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Louisiana and then calculated the number per adult Louisianan (see note 5) per month.

4. Roger Grimes, "[Smishing 101 and Defenses](#)," KnowBe4 (Jan. 8, 2020).

5. TrueCaller, "[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)" (2021). Truecaller's survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Louisiana's adult population (3,542,020 in 2021, per the [U.S. Census Bureau](#)) is 488,799.

Scam Robocalls in Maine

The FBI Boston Division, which oversees Maine, reported an increase in phone scammers who target New Englanders claiming to be representatives of a government agency, often threatening arrest unless immediate payments are made. In 2020, Mainers lost more than \$32,000 to these government impersonation scams.¹



But these are not the only robocall scams targeting Mainers. According to estimates based on data from YouMail, the most prevalent scam campaigns of January 2022 accounted for more than 1.8 million scam robocalls made to Maine phones in that month alone, and these top campaigns are only a portion of the total scam robocalls made.² **In 2021, Mainers received more than 130 million robocalls** (see Robocalls in Maine graph), **about 55 million (42%) of which were scam robocalls**—or about 4 scam robocalls for each Mainer per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, more than 150,000 Mainers lost money to scam robocalls in 2021.⁵

1. Dennis Hoey, “FBI warns of telephone scammers, posing as federal agents, who bilked 44 Mainers,” Portland Press Herald (April 21, 2021).

2. YouMail confidential data provided to NCLC. We multiplied the number of calls from the top 1,000 scam robocall campaigns nationwide in January by Maine’s share of the US adult population (0.4%) to estimate calls made to Maine phones in January.

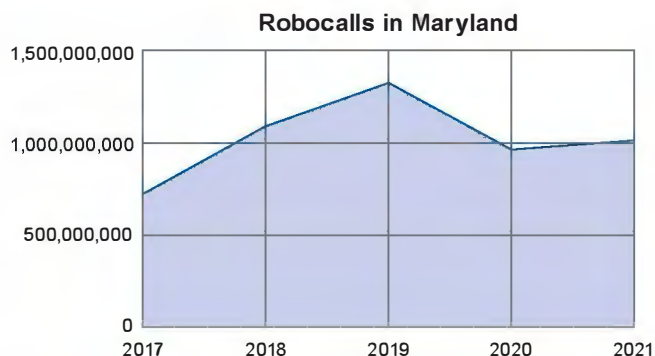
3. YouMail, “Historical Robocalls by State” (2022). YouMail, “U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index.” Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Maine and then calculated the number per adult Mainer (see note 5) per month.

4. Roger Grimes, “Smishing 101 and Defenses,” KnowBe4 (Jan. 8, 2020).

5. TrueCaller, “TrueCaller Insights 2021 U.S. Spam & Scam Report” (2021). Truecaller’s survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Maine’s adult population (1,118,381 in 2021, per the U.S. Census Bureau) is 154,337.

Scam Robocalls in Maryland

Maryland State Police warned residents of a robocall scam going around in which the scammer claims to be a law enforcement officer and threatens the victim with criminal charges. The calls are spoofed so that they appear to be coming from a legitimate law enforcement number.¹



This kind of scam is not rare. According to estimates based on data from YouMail, more than 83,000 scam “arrest warrant” robocalls were made to Maryland phones in January 2022 alone.² **In 2021, Marylanders received more than a billion robocalls** (see Robocalls in Maryland graph), **about 424 million (42%) of which were scam robocalls**—or about 7 scam robocalls for each Marylander per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, well over half a million Marylanders lost money to scam robocalls in 2021.⁵

1. Bryna Zumer, “[Scam Alert: New phone scam ‘spoofs’ Maryland State Police number](#),” Fox 45 News (Oct. 1, 2020).

2. YouMail confidential data provided to NCLC, filtered by campaigns related to arrest warrant scams. We multiplied nationwide scam arrest warrant robocalls in January by Maryland’s share of the US adult population (1.9%) to estimate calls made to Maryland phones in January.

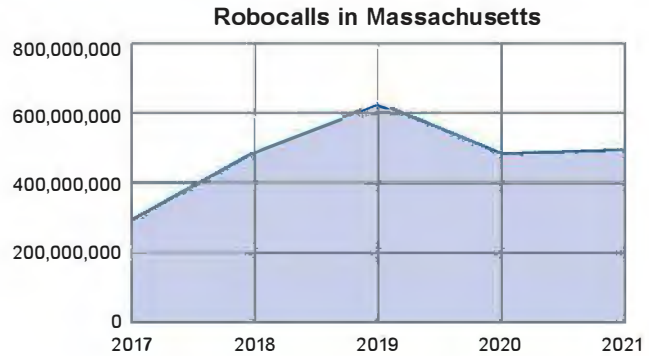
3. YouMail, “[Historical Robocalls by State](#)” (2022). YouMail, “[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#).” Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Maryland and then calculated the number per adult Marylander (see note 5) per month.

4. Roger Grimes, “[Smishing 101 and Defenses](#),” KnowBe4 (Jan. 8, 2020).

5. TrueCaller, “[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)” (2021). Truecaller’s survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Maryland’s adult population (4,802,635 in 2021, per the [U.S. Census Bureau](#)) is 662,764.

Scam Robocalls in Massachusetts

In 2021, an elderly Massachusetts woman received a robocall purporting to be from the Social Security Administration, telling her that her Social Security number was about to be “suspended” due to criminal activity. The scammers convinced the woman to send them \$900,000 from her bank and retirement accounts, in a scam that largely targeted elderly victims.¹



Sadly, this consumer is far from the only Bay Stater to encounter this kind of robocall scam. According to estimates based on data from YouMail, nearly 200,000 scam Social Security robocalls were made to Massachusetts phones in the month of January 2022 alone.² **In 2021, Massachusetts residents received nearly 500 million robocalls (see Robocalls in Massachusetts graph), 206 million (42%) of which were scam robocalls**—or about 3 scam robocalls for each Bay Stater per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, nearly 800,000 Massachusetts residents lost money to scam robocalls in 2021.⁵

1. Michelle Singletary, “I saved my sister from a Social Security scam. Listen to the actual call,” Washington Post (July 9, 2021).

2. YouMail confidential data provided to NCLC, filtered by campaigns related to Social Security scams. We multiplied nationwide scam Social Security robocalls in January by Massachusetts’ share of the US adult population (2.2%) to estimate calls made to Massachusetts phones in January.

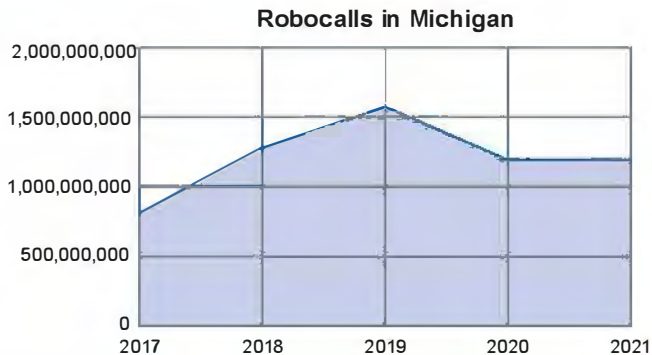
3. YouMail, “Historical Robocalls by State” (2022). YouMail, “U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index.” Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Massachusetts and then calculated the number per adult Bay Stater (see note 5) per month.

4. Roger Grimes, “Smishing 101 and Defenses,” KnowBe4 (Jan. 8, 2020).

5. TrueCaller, “TrueCaller Insights 2021 U.S. Spam & Scam Report” (2021). Truecaller’s survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Massachusetts’ adult population (5,615,717 in 2021, per the U.S. Census Bureau) is 774,969. Indeed, Bay Staters filed 3,491 complaints to law enforcement about scams caused by calls and text messages, reporting losses of over \$4.3 million in 2021. (This is an extrapolated figure, real data is coming from the FTC.)

Scam Robocalls in Michigan

Michigan's Attorney General is warning consumers of a new robocall scam in which the scammer, pretending to be from AT&T, offers the consumer a big discount on DirecTV. The scammer then demands payment up front using a gift card.¹



This kind of scam is not rare.

According to estimates based on data from YouMail, more than 600,000 business impersonation scam robocalls were made to Michigan phones in January 2022 alone.² **In 2021, Michiganders received more than 1.2 billion robocalls** (see Robocalls in Michigan graph), **about 500 million (42%) of which were scam robocalls**—or about 5 scam robocalls for each Michigander per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, more than a million Michiganders lost money to scam robocalls in 2021.⁵

1. Derick Hutchinson, "[Do you get those annoying 'AT&T DirecTV' robocalls? Michigan's AG is trying to stop them](#)," ClickOnDetroit (Feb. 17, 2022).

2. YouMail confidential data provided to NCLC, filtered by campaigns related to business impersonation scams. We multiplied nationwide scam business impersonation robocalls in January by Michigan's share of the US adult population (3.1%) to estimate calls made to Michigan phones in January.

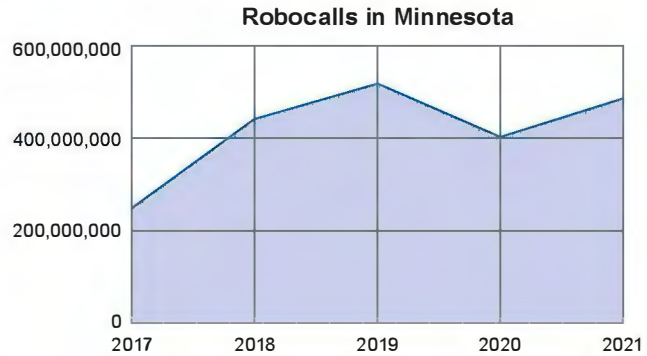
3. YouMail, "[Historical Robocalls by State](#)" (2022). YouMail, "[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#)." Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Michigan and then calculated the number per adult Michigander (see note 5) per month.

4. Roger Grimes, "[Smishing 101 and Defenses](#)," KnowBe4 (Jan. 8, 2020).

5. TrueCaller, "[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)" (2021). Truecaller's survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Michigan's adult population (7,889,887 in 2021, per the U.S. Census Bureau) is 1,088,804.

Scam Robocalls in Minnesota

Last year a massive phone scam operating out of Minnesota that had stolen \$300 million from consumers across the nation, was shut down by federal officials.¹ Although this is good news for the victims of the scam, the problem of fraudulent robocalls is far from over.



According to estimates based on data from YouMail, the most prevalent scam campaigns of January 2022 accounted for nearly 7.8 million scam robocalls made to Minnesota phones in that month alone, and these top campaigns are only a portion of the total scam robocalls made.² **In 2021, Minnesotans received nearly 500 million robocalls** (see Robocalls in Minnesota graph), **about 200 million (42%) of which were scam robocalls**—or between 3 and 4 scam robocalls for each Minnesotan per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, well over half a million Minnesotans lost money to scam robocalls in 2021.⁵

1. Lauren Leamenczyk, "[Inside one of Minnesota's biggest phone scams](#)," KARE 11 (May 12, 2021).

2. YouMail confidential data provided to NCLC. We multiplied the number of calls from the top 1,000 scam robocall campaigns nationwide in January by Minnesota's share of the US adult population (1.7%) to estimate calls made to Minnesota phones in January.

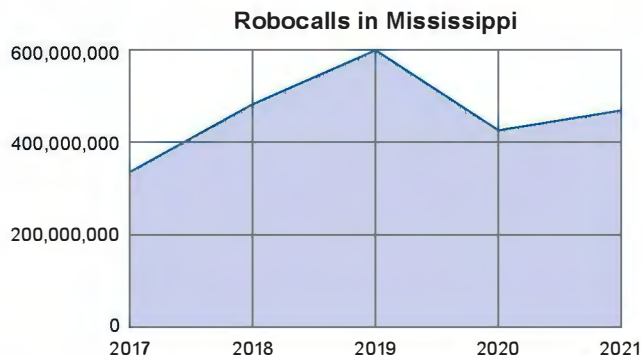
3. YouMail, "[Historical Robocalls by State](#)" (2022). YouMail, "[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#)." Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Minnesota and then calculated the number per adult Minnesotan (see note 5) per month.

4. Roger Grimes, "[Smishing 101 and Defenses](#)," KnowBe4 (Jan. 8, 2020).

5. TrueCaller, "[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)" (2021). Truecaller's survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Minnesota's adult population (4,388,983 in 2021, per the [U.S. Census Bureau](#)) is 605,680.

Scam Robocalls in Mississippi

Last year the Mississippi Public Service Commission warned residents of a vehicle warranty robocall scam making the rounds. Scammers used public state motor vehicle records to convince victims that their warranty was about to expire, but that they could renew it—for a fee.¹



But this was not the only robocall scam targeting Mississippians. According to estimates based on data from YouMail, more than a million scam “vehicle warranty” robocalls were made to Mississippi phones in January 2022 alone.² **In 2021, Mississippians received 470 million robocalls** (see Robocalls in Mississippi graph), **nearly 200 million (42%) of which were scam robocalls**—or about 7 scam robocalls for each Mississippian per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, well over a quarter million Mississippians lost money to scam robocalls in 2021.⁵

1. Brent Bailey, “[Scam calls overload: Auto warranties](#),” MS Public Service Commission (May 26, 2021).

2. YouMail confidential data provided to NCLC. We multiplied the number of calls from the top 1,000 scam robocall campaigns nationwide in January by Mississippi’s share of the US adult population (0.9%) to estimate calls made to Mississippi phones in January.

3. YouMail, “[Historical Robocalls by State](#)” (2022). YouMail, “[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#).” Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Mississippi and then calculated the number per adult Mississippian (see note 5) per month.

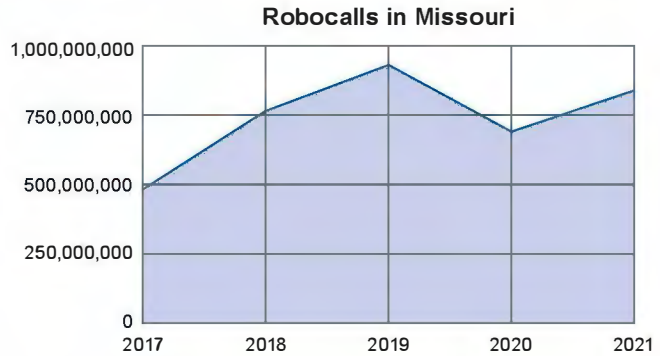
4. Roger Grimes, “[Smishing 101 and Defenses](#),” KnowBe4 (Jan. 8, 2020).

5. TrueCaller, “[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)” (2021). Truecaller’s survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Mississippi’s adult population (2,256,723 in 2021, per the [U.S. Census Bureau](#)) is 311,428.

Scam Robocalls in Missouri

The Missouri Attorney General warned residents of an Apple Support robocall scam. Scammers attempt to obtain money or personal information from their victims.¹

This kind of scam is not rare. According to estimates based on data from YouMail, more than 370,000 business impersonation scam robocalls were made to Missouri phones in January 2022 alone.² **In 2021, Missourians received more than 830 million robocalls** (see Robocalls in Missouri graph), **350 million (42%) of which were scam robocalls**—or about 6 scam robocalls for each Missourian per month.³ An Assistant Attorney General reported that robocalls are “the number one complaint that our office receives.”⁴ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁵



These robocalls have a cost. According to estimates based on TrueCaller survey data, more than 660,000 Missourians lost money to scam robocalls in 2021.⁶

1. ON YOUR SIDE CONSUMER ALERT: [Missouri atty. gen. warns of fraudulent Apple support calls](#), KY3 (Oct. 31, 2019).

2. YouMail confidential data provided to NCLC. We multiplied the number of calls from the top 1,000 scam robocall campaigns nationwide in January by Missouri’s share of the US adult population (1.9%) to estimate calls made to Missouri phones in January.

3. YouMail, “[Historical Robocalls by State](#)” (2022). YouMail, “[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#).” Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Missouri and then calculated the number per adult Missourian (see note 6) per month.

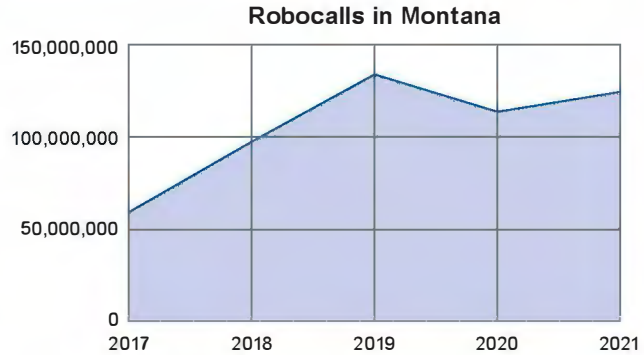
4. Holden Kurwicki, “[Missouri attorney general’s office cracking down on robocalls, spam texts](#),” KSDK-TV (March 30, 2022).

5. Roger Grimes, “[Smishing 101 and Defenses](#),” KnowBe4 (Jan. 8, 2020).

6. TrueCaller, “[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)” (2021). Truecaller’s survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Missouri’s adult population (4,792,681 in 2021, per the U.S. Census Bureau) is 661,390.

Scam Robocalls in Montana

Last year Montana’s Department of Justice warned residents against robocall scams related to the pandemic. One elderly Montana couple fell victim to scammers who convinced them to go out in a snowstorm to withdraw money. On the way, their car crashed, and the husband died.¹



Robocall scams are a huge and growing problem. According to estimates based on data from YouMail, more than 1.3 million scam robocalls were made to Montana phones in January 2022 alone.² **In 2021, Montanans received 124 million robocalls** (see Robocalls in Montana graph), **about 52 million (42%) of which were scam robocalls**—or about 5 scam robocalls for each Montanan per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, nearly 120,000 Montanans lost money to scam robocalls in 2021.⁵

1. Colter Anstaett, “[FTC warns of scammers trying to take advantage of COVID fears](#),” KRTV 3 (March 24, 2021).

2. YouMail confidential data provided to NCLC. We multiplied the number of calls from the top 1,000 scam robocall campaigns nationwide in January by Montana’s share of the US adult population (0.3%) to estimate calls made to Montana phones in January.

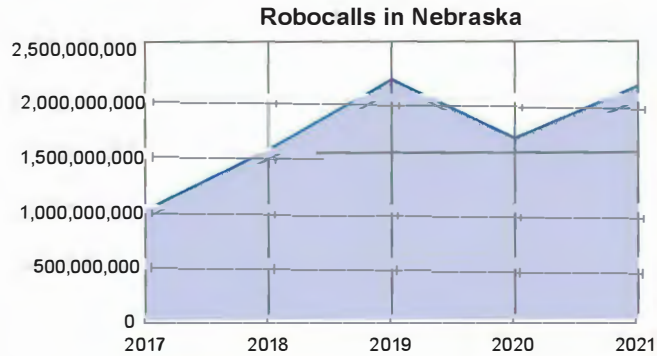
3. YouMail, “[Historical Robocalls by State](#)” (2022). YouMail, “[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#).” Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Montana and then calculated the number per adult Montanan (see note 5) per month.

4. Roger Grimes, “[Smishing 101 and Defenses](#),” KnowBe4 (Jan. 8, 2020).

5. TrueCaller, “[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)” (2021). Truecaller’s survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Montana’s adult population (867,957 in 2021, per the [U.S. Census Bureau](#)) is 119,778.

Scam Robocalls in Nebraska

Last year Nebraska’s Drug Enforcement Administration office warned residents of a robocall scam in which scammers posed as agents. Scammers would attempt to steal victims’ personal or financial information or money while threatening arrest.¹



This robocall scam is far from rare. According to estimates

based on data from YouMail, more than 26,000 scam “arrest warrant” robocalls were made to Nebraska phones in January 2022 alone.² **In 2021, Nebraskans received 210 million robocalls** (see Robocalls in Nebraska graph), **about 88 million (42%) of which were scam robocalls**—or about 5 scam robocalls for each Nebraskan per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, more than 200,000 Nebraskans lost money to scam robocalls in 2021.⁵

1. KMTV 3, “[Omaha DEA warns scammers posing as agents to steal identities](#)” (March 31, 2021).

2. YouMail confidential data provided to NCLC, filtered by campaigns related to arrest warrant scams. We multiplied nationwide scam arrest warrant robocalls in January by Nebraska’s share of the US adult population (0.6%) to estimate calls made to Nebraska phones in January.

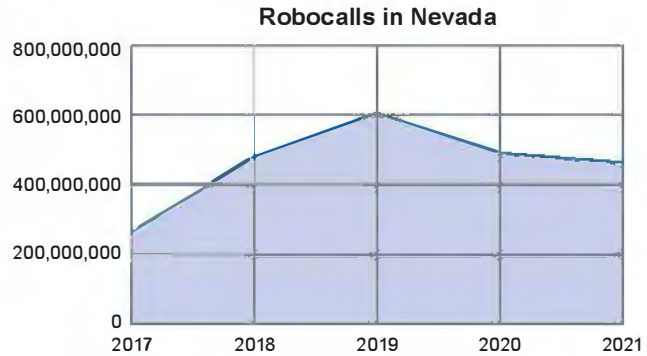
3. YouMail, “[Historical Robocalls by State](#)” (2022). YouMail, “[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#).” Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Nebraska and then calculated the number per adult Nebraskan (see note 5) per month.

4. Roger Grimes, “[Smishing 101 and Defenses](#),” KnowBe4 (Jan. 8, 2020).

5. TrueCaller, “[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)” (2021). Truecaller’s survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Nebraska’s adult population (1,480,624 in 2021, per the [U.S. Census Bureau](#)) is 204,326.

Scam Robocalls in Nevada

Last year, Nevada’s Attorney General took action against a huge robocall scam operation, which had made more than a billion fake “charitable fundraising” robocalls and stolen \$110 million from its victims.¹ While this particular scam operation has been shut down, the problem of fraudulent robocalls continues. Nevada receives the sixth-highest number of robocalls per state in the country, by some estimates.²



According to estimates based on data from YouMail, the most prevalent scam campaigns of January 2022 accounted for more than 4.1 million scam robocalls made to Nevada phones in that month alone, and these top campaigns are only a portion of the total scam robocalls made.³ **In 2021, Nevadans received about 460 million robocalls** (see Robocalls in Nevada graph), **nearly 200 million (42%) of which were scam robocalls**—or between 6 and 7 scam robocalls for each Nevadan per month.⁴ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁵

These robocalls have a cost. According to estimates based on TrueCaller survey data, well over a quarter million Nevadans lost money to scam robocalls in 2021.⁶

1. Bryan Horwath, “Do not call: Combating illegal robocalls tricky, Nevada official says,” Las Vegas Sun (April 20, 2021).

2. Id.

3. YouMail confidential data provided to NCLC. We multiplied the number of calls from the top 1,000 scam robocall campaigns nationwide in January by Nevada’s share of the US adult population (0.9%) to estimate calls made to Nevada phones in January.

4. YouMail, “Historical Robocalls by State” (2022). YouMail, “U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index.” Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Nevada and then calculated the number per adult Nevadan (see note 6) per month.

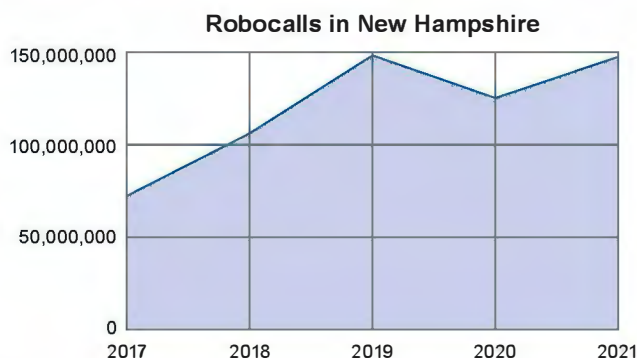
5. Roger Grimes, “Smishing 101 and Defenses,” KnowBe4 (Jan. 8, 2020).

6. TrueCaller, “TrueCaller Insights 2021 U.S. Spam & Scam Report” (2021). Truecaller’s survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Nevada’s adult population (2,436,593 in 2021, per the U.S. Census Bureau) is 336,250.

Scam Robocalls in New Hampshire

New Hampshire's Attorney General earlier this year joined with other state AGs in urging the FCC to take action against the flood of foreign scam robocalls victimizing consumers in New Hampshire and across the country.¹

According to estimates based on data from YouMail, the most prevalent scam campaigns of January 2022 accounted for more than 1.8 million scam robocalls made to New Hampshire phones over that period alone, and these top campaigns are only a portion of the total scam robocalls made.² **In 2021, New Hampshire residents received nearly 150 million robocalls** (see Robocalls in New Hampshire graph), **over 60 million (42%) of which were scam robocalls**—or between 4 and 5 scam robocalls for each New Hampshire resident per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴



These robocalls have a cost. According to estimates based on TrueCaller survey data, more than 150,000 New Hampshire residents lost money to scam robocalls in 2021.⁵

1. [Robocall Scammers Target NH Taxpayers](#), BusinessNH Magazine (Mar. 7, 2019).

2. YouMail confidential data provided to NCLC. We multiplied the number of calls from the top 1,000 scam robocall campaigns nationwide in January by New Hampshire's share of the US adult population (0.4%) to estimate calls made to New Hampshire phones in January.

3. YouMail, "[Historical Robocalls by State](#)" (2022). YouMail, "[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#)." Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in New Hampshire and then calculated the number per adult New Hampshire resident (see note 5) per month.

4. Roger Grimes, "[Smishing 101 and Defenses](#)," KnowBe4 (Jan. 8, 2020).

5. TrueCaller, "[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)" (2021). Truecaller's survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of New Hampshire's adult population (1,127,862 in 2021, per the [U.S. Census Bureau](#)) is 155,645.

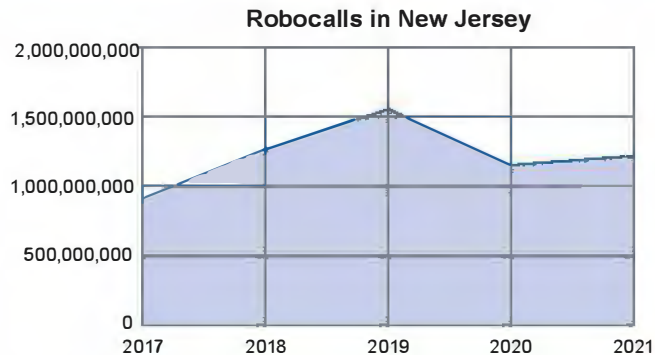
Scam Robocalls in New Jersey

The Garden State leads the nation in resident complaints about robocalls. In 2022, New Jersey's Attorney General announced a partnership with the FCC to combat illegal and fraudulent robocalls.¹

According to estimates based on data from YouMail, the most prevalent scam campaigns of

January 2022 accounted for more than 12.8 million scam robocalls made to New Jersey phones in January 2022 alone, and these top campaigns are only a portion of the total scam robocalls made.² **In 2021, New Jerseyans received more than 1.2 billion robocalls** (see Robocalls in New Jersey graph), **more than 500 million (42%) of which were scam robocalls**—or between 5 and 6 scam robocalls for each New Jerseyan per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, more than a million New Jerseyans lost money to scam robocalls in 2021.⁵



1. Krystal Knapp, "[New Jersey to work with FCC on robocall investigations](#)," Planet Princeton (March 28, 2022).

2. YouMail confidential data provided to NCLC. We multiplied the number of calls from the top 1,000 scam robocall campaigns nationwide in January by New Jersey's share of the US adult population (2.8%) to estimate calls made to New Jersey phones in January.

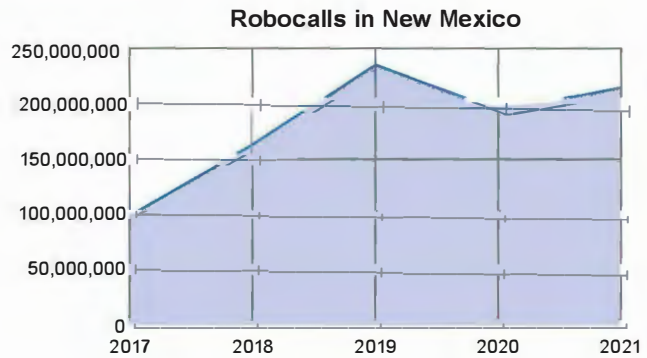
3. YouMail, "[Historical Robocalls by State](#)" (2022). YouMail, "[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#)." Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in New Jersey and then calculated the number per adult New Jerseyan (see note 5) per month.

4. Roger Grimes, "[Smishing 101 and Defenses](#)," KnowBe4 (Jan. 8, 2020).

5. TrueCaller, "[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)" (2021). Truecaller's survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of New Jersey's adult population (7,246,896 in 2021, per the [U.S. Census Bureau](#)) is 1,000,072.

Scam Robocalls in New Mexico

Scammers claiming to be federal agents are targeting consumers in New Mexico, often spoofing their phone numbers so that the calls appear to come from an official District Court of New Mexico number. The victims are told that they are “under investigation,” or that a warrant has been issued for their arrest, and that they must make immediate payments to resolve the matter.¹



This robocall scam is far from rare. According to estimates based on data from YouMail, more than 26,000 scam “arrest warrant” robocalls were made to New Mexico phones in January 2022 alone.² **In 2021, New Mexicans received more than 215 million robocalls** (see Robocalls in New Mexico graph), **over 90 million (42%) of which were scam robocalls**—or between 4 and 5 scam robocalls for each New Mexican per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, nearly a quarter million New Mexicans lost money to scam robocalls in 2021.⁵

1. U.S. District Court of New Mexico, “[Warning: Scam phone calls received by individuals from the public in the District of New Mexico](#)” (June 26, 2020).

2. YouMail confidential data provided to NCLC, filtered by campaigns related to arrest warrant scams. We multiplied nationwide scam arrest warrant robocalls in January by New Mexico’s share of the US adult population (0.6%) to estimate calls made to New Mexico phones in January.

3. YouMail, “[Historical Robocalls by State](#)” (2022). YouMail, “[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#).” Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in New Mexico and then calculated the number per adult New Mexican (see note 5) per month.

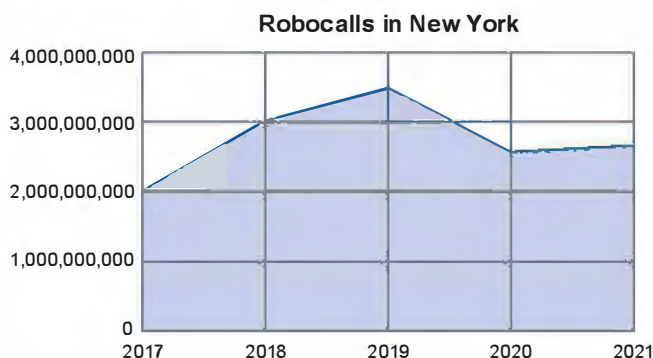
4. Roger Grimes, “[Smishing 101 and Defenses](#),” KnowBe4 (Jan. 8, 2020).

5. TrueCaller, “[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)” (2021). Truecaller’s survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of New Mexico’s adult population (1,635,573 in 2021, per the [U.S. Census Bureau](#)) is 225,709.

Scam Robocalls in New York

Last year New York’s governor signed into law two measures aimed at combating robocalls. However, their prospects of impacting the growing scam robocall problem are uncertain.¹

According to estimates based on data from YouMail, the most prevalent scam campaigns of January 2022 accounted for nearly 28 million scam robocalls made to New York phones in that month alone, and these top campaigns are only a portion of the total scam robocalls made.² **In 2021, New Yorkers received more than 2.6 billion robocalls** (see Robocalls in New York graph), **over 1 billion (42%) of which were scam robocalls**—or more than 5 scam robocalls for each New Yorker per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴



These robocalls have a cost. According to estimates based on TrueCaller survey data, more than 2 million New Yorkers lost money to scam robocalls in 2021.⁵

1. Jake Offenhardt, “NY moves to crack down on robocalls. Don’t expect the scammers to go quietly,” Gothamist (Nov. 8, 2021).

2. YouMail confidential data provided to NCLC. We multiplied the number of calls from the top 1,000 scam robocall campaigns nationwide in January by New York’s share of the US adult population (6.1%) to estimate calls made to New York phones in January.

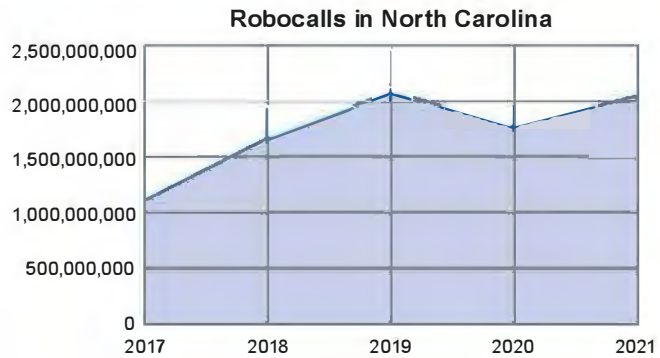
3. YouMail, “Historical Robocalls by State” (2022). YouMail, “U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index.” Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in New York and then calculated the number per adult New Yorker (see note 5) per month.

4. Roger Grimes, “Smishing 101 and Defenses,” KnowBe4 (Jan. 8, 2020).

5. TrueCaller, “TrueCaller Insights 2021 U.S. Spam & Scam Report” (2021). Truecaller’s survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of New York’s adult population (15,729,879 in 2021, per the U.S. Census Bureau) is 2,170,723.

Scam Robocalls in North Carolina

North Carolina's Attorney General recently reported that phone scams, and especially robocall scams, are by far the most common type of scam reported to his office. Telemarketing and robocall scams made up more than a third of all complaints in 2021.¹



According to estimates based on data from YouMail, the most prevalent scam campaigns of January 2022 accounted for more than 14.6 million scam robocalls made to North Carolina phones in that month alone, and these top campaigns are only a portion of the total scam robocalls made.² **In 2021, North Carolinians received more than 2 billion robocalls (see Robocalls in North Carolina graph), nearly 860 million (42%) of which were scam robocalls**—or between 8 and 9 scam robocalls for each North Carolinian per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, more than a million North Carolinians lost money to scam robocalls in 2021.⁵

1. Matthew Ablon, "[These are the most-reported scams in North Carolina from 2021 according to the state Attorney General's office](#)," WCNC Charlotte (Jan. 19, 2022).

2. YouMail confidential data provided to NCLC. We multiplied the number of calls from the top 1,000 scam robocall campaigns nationwide in January by North Carolina's share of the US adult population (3.2%) to estimate calls made to North Carolina phones in January.

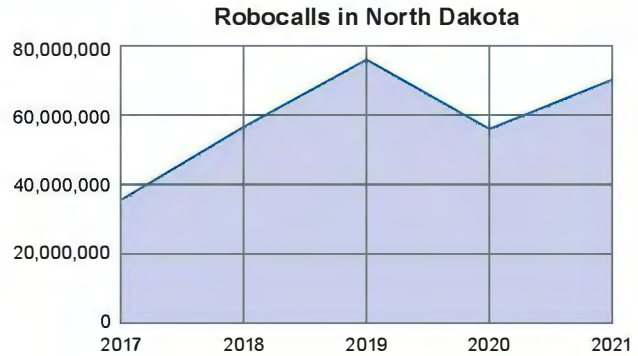
3. YouMail, "[Historical Robocalls by State](#)" (2022). YouMail, "[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#)." Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in North Carolina and then calculated the number per adult North Carolinian (see note 5) per month.

4. Roger Grimes, "[Smishing 101 and Defenses](#)," KnowBe4 (Jan. 8, 2020).

5. TrueCaller, "[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)" (2021). Truecaller's survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of North Carolina's adult population (8,240,458 in 2021, per the [U.S. Census Bureau](#)) is 1,137,183.

Scam Robocalls in North Dakota

A North Dakota sheriff's department warned residents of scammers claiming to be sheriff's deputies and threatening arrest. The sheriff's department warns North Dakotans never to pay "fines" or "bonds" over the phone, and especially never to pay anything to a person asking for payment in gift cards.¹



Robocall scams like this "arrest warrant" scam represent thousands of calls made to North Dakotans each month. According to estimates based on data from YouMail, nearly 9,000 scam "arrest warrant" robocalls were made to North Dakota phones in January 2022 alone.² **In 2021, North Dakotans received more than 70 million robocalls** (see Robocalls in North Dakota graph), **nearly 30 million (42%) of which were scam robocalls**—or about 4 scam robocalls for each North Dakotan per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, more than 80,000 North Dakotans lost money to scam robocalls in 2021.⁵

1. Joe Skurzewski, "[Ward County Sheriff's Department warns residents of phone scam](#)," KFYZ TV (Dec. 5, 2021).

2. YouMail confidential data provided to NCLC, filtered by campaigns related to arrest warrant scams. We multiplied nationwide scam arrest warrant robocalls in January by North Dakota's share of the US adult population (0.2%) to estimate calls made to North Dakota phones in January.

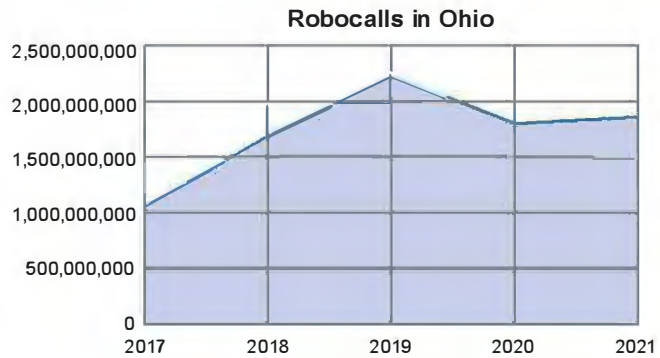
3. YouMail, "[Historical Robocalls by State](#)" (2022). YouMail, "[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#)." Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in North Dakota and then calculated the number per adult North Dakotan (see note 5) per month.

4. Roger Grimes, "[Smishing 101 and Defenses](#)," KnowBe4 (Jan. 8, 2020).

5. TrueCaller, "[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)" (2021). Truecaller's survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of North Dakota's adult population (592,060 in 2021, per the [U.S. Census Bureau](#)) is 81,704.

Scam Robocalls in Ohio

The Ohio Attorney General issued a warning in 2021 about illegal robocallers posing as Amazon, Apple, or PayPal representatives. Scammers would attempt to persuade consumers to buy gift cards as a way of “stopping” unauthorized purchases or attempt to gain access to the consumer’s account by pretending to issue a refund.¹



Unfortunately, this kind of robocall scam is not rare. According to estimates based on data from YouMail, more than 506,000 scam “fraud alert” robocalls were made to Ohio phones in January 2022 alone.² **In 2021, Ohioans received nearly 2 billion robocalls** (see Robocalls in Ohio graph), **nearly 800 million (42%) of which were scam robocalls**—or about 7 scam robocalls for each Ohioan per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, more than 1.2 million Ohioans lost money to scam robocalls in 2021.⁵

1. WTVG, “Ohio AG warning of new phone scams,” (Nov. 22, 2021).

2. YouMail confidential data provided to NCLC, filtered by campaigns related to fraud alerts. We multiplied nationwide scam fraud alert robocalls in January by Ohio’s share of the US adult population (3.6%) to estimate calls made to Ohio phones in January.

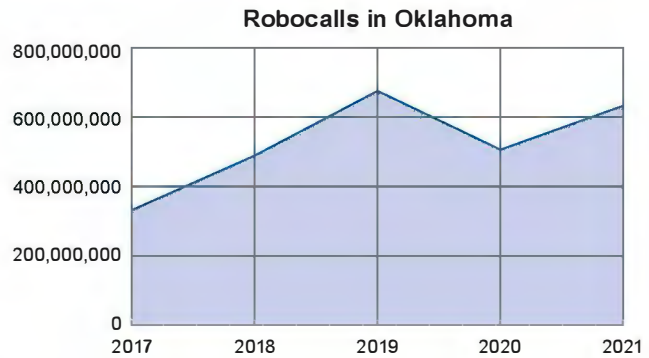
3. YouMail, “Historical Robocalls by State” (2022). YouMail, “U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index.” Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Ohio and then calculated the number per adult Ohioan (see note 5) per month.

4. Roger Grimes, “Smishing 101 and Defenses,” KnowBe4 (Jan. 8, 2020).

5. TrueCaller, “TrueCaller Insights 2021 U.S. Spam & Scam Report” (2021). Truecaller’s survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Ohio’s adult population (9,176,633 in 2021, per the U.S. Census Bureau) is 1,266,375.

Scam Robocalls in Oklahoma

Dana Loomer of Tulsa receives 10 to 15 robocalls per day. She blocks each number as it comes, but the spoofed robocalls just keep coming from different numbers. “I’ve probably got a hundred phone numbers blocked, and they just keep coming up with new ones,” she said.¹



Dana isn’t alone in dealing with a tidal wave of robocalls. According to estimates based on data from YouMail, the most prevalent scam campaigns of January 2022 accounted for more than 5.5 million scam robocalls made to Oklahoma phones in that month alone, and these top campaigns are only a portion of the total scam robocalls made.² **In 2021, Oklahomans received more than 600 million robocalls** (see Robocalls in Oklahoma graph), **over 260 million (42%) of which were scam robocalls**—or about 7 scam robocalls for each Oklahoman per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, more than 400,000 Oklahomans lost money to scam robocalls in 2021.⁵

1. Katie Keleher, “[Many frustrated with high numbers of robocalls](#),” 2 News Oklahoma (March 24, 2021).

2. YouMail confidential data provided to NCLC. We multiplied the number of calls from the top 1,000 scam robocall campaigns nationwide in January by Oklahoma’s share of the US adult population (1.2%) to estimate calls made to Oklahoma phones in January.

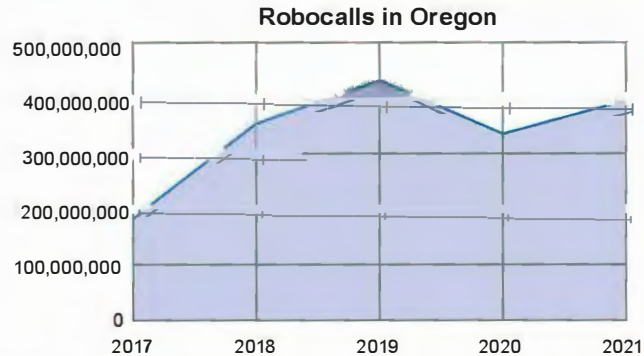
3. YouMail, “[Historical Robocalls by State](#)” (2022). YouMail, “[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#).” Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Oklahoma and then calculated the number per adult Oklahoman (see note 5) per month.

4. Roger Grimes, “[Smishing 101 and Defenses](#),” KnowBe4 (Jan. 8, 2020).

5. TrueCaller, “[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)” (2021). Truecaller’s survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Oklahoma’s adult population (3,025,859 in 2021, per the [U.S. Census Bureau](#)) is 417,569.

Scam Robocalls in Oregon

Telecommunications scams are one of the most common types reported to Oregon's Department of Justice.¹ Last year, the Oregon Department of Motor Vehicles (DMV) reported a text scam impersonating the DMV, in which scammers try to get payment information from unsuspecting Oregonians.²



But these are not the only telecommunications scams targeting Oregonians. According to estimates based on data from YouMail, the most prevalent scam robocall campaigns of January 2022 accounted for nearly 6 million scam robocalls made to Oregon phones in that month alone, and these campaigns are only a portion of the total scam robocalls made.³ **In 2021, Oregonians received nearly 400 million robocalls (see Robocalls in Oregon graph), over 160 million (42%) of which were scam robocalls**—or about 4 scam robocalls for each Oregonian per month.⁴ As evidenced by the DMV example, calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁵

These robocalls have a cost. According to estimates based on TrueCaller survey data, nearly half a million Oregonians lost money to scam robocalls in 2021.⁶

1. Demi Lawrence, "[The top scams and phony calls that fuel Oregon consumer complaints](#)," KGW8 (March 9, 2022).

2. [Don't Be Fooled: Oregon DMV warns of new text scam](#), The Chronicle Online.com (Nov. 30, 2021, updated Mar. 3, 2022).

3. YouMail confidential data provided to NCLC. We multiplied the number of calls from the top 1,000 scam robocall campaigns nationwide in January by Oregon's share of the US adult population (1.3%) to estimate calls made to Oregon phones in January.

4. YouMail, "[Historical Robocalls by State](#)" (2022). YouMail, "[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#)." Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Oregon and then calculated the number per adult Oregonian (see note 6) per month.

5. Roger Grimes, "[Smishing 101 and Defenses](#)," KnowBe4 (Jan. 8, 2020).

6. TrueCaller, "[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)" (2021). Truecaller's survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Oregon's adult population (3,375,693 in 2021, per the [U.S. Census Bureau](#)) is 465,846.

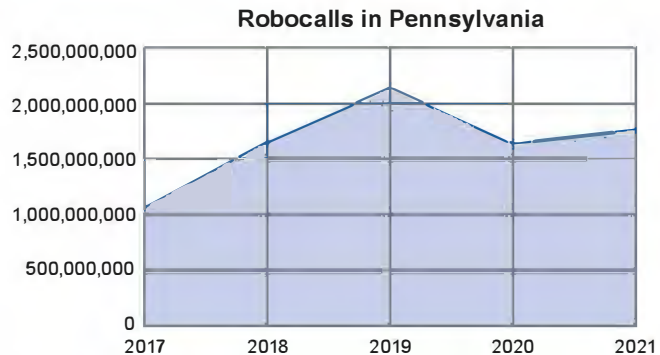
Scam Robocalls in Pennsylvania

Pennsylvania ranks 15th among the 50 states for unwanted call complaints filed with the Do Not Call Registry over the last several years. However, consumer complaints only capture a fraction of the problem.¹

According to estimates based on data from YouMail, the most prevalent scam campaigns of

January 2022 accounted for more than 18.3 million scam robocalls were made to Pennsylvania phones in that month alone, and these top campaigns are only a portion of the total scam robocalls made.² **In 2021, Pennsylvanians received more than 1.7 billion robocalls** (see Robocalls in Pennsylvania graph), **over 735 million (42%) of which were scam robocalls**—or nearly 6 scam robocalls for each Pennsylvanian per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, more than 1.4 million Pennsylvanians lost money to scam robocalls in 2021.⁵



1. David Bruce, "[Erie County residents tired of robocalls, telemarketing calls](#)," Erie Times-News (Dec. 2, 2021).

2. YouMail confidential data provided to NCLC. We multiplied the number of calls from the top 1,000 scam robocall campaigns nationwide in January by Pennsylvania's share of the US adult population (4.0%) to estimate calls made to Pennsylvania phones in January.

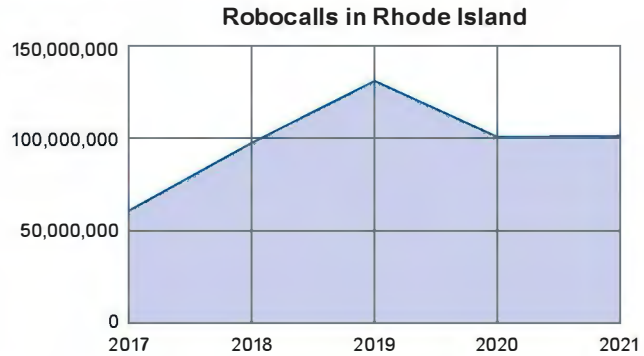
3. YouMail, "[Historical Robocalls by State](#)" (2022). YouMail, "[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#)." Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Pennsylvania and then calculated the number per adult Pennsylvanian (see note 5) per month.

4. Roger Grimes, "[Smishing 101 and Defenses](#)," KnowBe4 (Jan. 8, 2020).

5. TrueCaller, "[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)" (2021). Truecaller's survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Pennsylvania's adult population (10,293,460 in 2021, per the [U.S. Census Bureau](#)) is 1,420,498.

Scam Robocalls in Rhode Island

The FBI Boston Division, which oversees Rhode Island, is seeing an increase in phone scammers who target New Englanders claiming to be representatives of a government agency, often threatening arrest unless immediate payments are made. In 2020, Rhode Islanders lost more than \$412,000 to these government impersonation scams.¹



But these are not the only robocall scams targeting Rhode Islanders. According to estimates based on data from YouMail, more than 13,000 scam “arrest warrant” robocalls were made to Rhode Island phones in January 2022 alone.² **In 2021, Rhode Islanders received more than 100 million robocalls (see Robocalls in Rhode Island graph), over 43 million (42%) of which were scam robocalls**—or more than 4 scam robocalls for each Rhode Islander per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, more than 120,000 Rhode Islanders lost money to scam robocalls in 2021.⁵

1. Kristin Setera, “[FBI warns public to beware of government impersonation scams](#),” FBI Boston (April 21, 2021).

2. YouMail confidential data provided to NCLC, filtered by campaigns related to arrest warrants. We multiplied nationwide scam arrest warrant robocalls in a January by Rhode Island’s share of the US adult population (0.3%) to estimate calls made to Rhode Island phones in January.

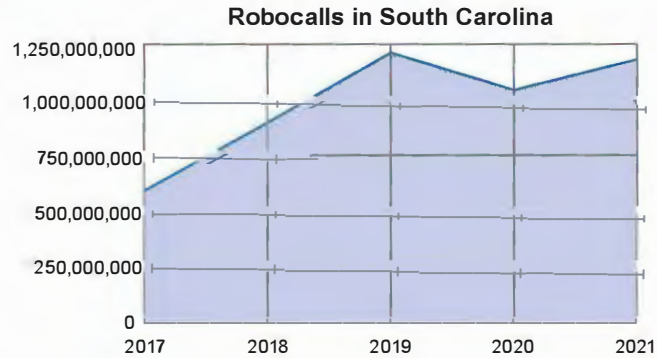
3. YouMail, “[Historical Robocalls by State](#)” (2022). YouMail, “[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#).” Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Rhode Island and then calculated the number per adult Rhode Islander (see note 5) per month.

4. Roger Grimes, “[Smishing 101 and Defenses](#),” KnowBe4 (Jan. 8, 2020).

5. TrueCaller, “[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)” (2021). Truecaller’s survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Rhode Island’s adult population (884,157 in 2021, per the [U.S. Census Bureau](#)) is 122,014.

Scam Robocalls in South Carolina

The South Carolina Attorney General has called robocalls “one of the most aggravating nuisances on earth.” Earlier this year, he joined the nation’s attorneys general in a letter to the FCC calling for stricter caller ID authentication to stem the tide of illegal robocalls, including scam robocalls.¹



According to estimates based on data from YouMail, the most prevalent scam campaigns of January 2022 accounted for more than 7.3 million scam robocalls made to South Carolina phones in that month alone, and these top campaigns are only a portion of the total scam robocalls made.² **In 2021, South Carolinians received nearly 1.2 billion robocalls (see Robocalls in South Carolina graph), almost 500 million (42%) of which were scam robocalls**—or about 10 scam robocalls for each South Carolinian per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, more than half a million South Carolinians lost money to scam robocalls in 2021.⁵

1. South Carolina Office of the Attorney General, “[Attorney General Alan Wilson works to stop international scam calls](#)” (Jan. 11, 2022).

2. YouMail confidential data provided to NCLC. We multiplied the number of calls from the top 1,000 scam robocall campaigns nationwide in January by South Carolina’s share of the US adult population (1.6%) to estimate calls made to South Carolina phones in January.

3. YouMail, “[Historical Robocalls by State](#)” (2022). YouMail, “[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#).” Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in South Carolina and then calculated the number per adult South Carolinian (see note 5) per month.

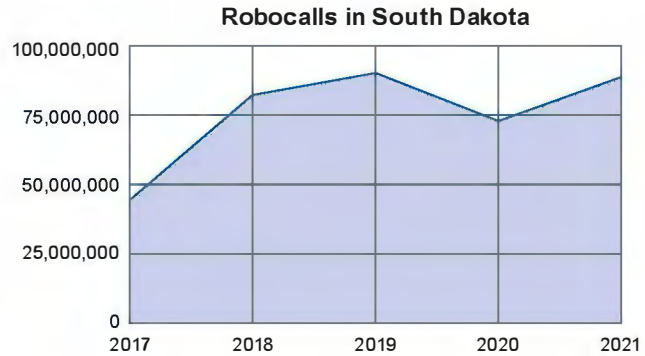
4. Roger Grimes, “[Smishing 101 and Defenses](#),” KnowBe4 (Jan. 8, 2020).

5. TrueCaller, “[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)” (2021). Truecaller’s survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of South Carolina’s adult population (4,069,513 in 2021, per the [U.S. Census Bureau](#)) is 561,593.

Scam Robocalls in South Dakota

In March 2021, the Attorney General’s Division of Consumer Protection issued an alert advising all South Dakotans to be cautious of phone calls claiming to be from Medicare, noting that reports of scam callers claiming to be with Medicare have been increasing. These callers ask individuals to verify their current

Medicare number on the premise that a new card and new number will be issued to the consumer. The Attorney General’s office advised that Medicare will never contact residents by phone, nor ask for personal identifying information.¹



This kind of scam is far from rare. According to estimates based on data from YouMail, more than 76,000 scam “Medicare” robocalls were made to South Dakota phones in January 2022 alone.² **In 2021, South Dakotans received more than 88 million robocalls** (see Robocalls in South Dakota graph), **about 37 million (42%) of which were scam robocalls**—or between 4 and 5 scam robocalls for each South Dakotan per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, nearly 100,000 South Dakotans lost money to scam robocalls in 2021.⁵

1. South Dakota Consumer Protection, “[Be alert for potential Medicare scam](#),” Office of the Attorney General (March 12, 2021).

2. YouMail confidential data provided to NCLC, filtered by campaigns related to Medicare. We multiplied nationwide scam Medicare robocalls in January by South Dakota’s share of the US adult population (0.3%) to estimate calls made to South Dakota phones in January.

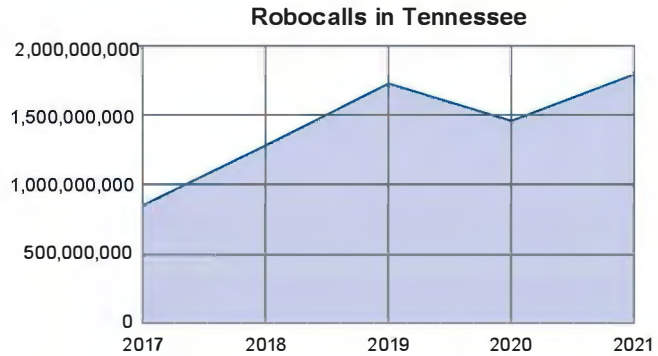
3. YouMail, “[Historical Robocalls by State](#)” (2022). YouMail, “[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#).” Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in South Dakota and then calculated the number per adult South Dakotan (see note 5) per month.

4. Roger Grimes, “[Smishing 101 and Defenses](#),” KnowBe4 (Jan. 8, 2020).

5. TrueCaller, “[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)” (2021). Truecaller’s survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of South Dakota’s adult population (676,009 in 2021, per the [U.S. Census Bureau](#)) is 93,289.

Scam Robocalls in Tennessee

Last year, Tennessee’s Attorney General helped to shut down a nationwide scam “charitable fundraising” organization that made over a billion robocalls and stole \$110 million from consumers. Some families received multiple robocalls per week from this single campaign.¹



Although this particular scam operation has been shut down, the problem of fraudulent robocalls continues. According to estimates based on data from YouMail, the most prevalent scam campaigns of January 2022 accounted for more than 9.6 million scam robocalls made to Tennessee phones in that month alone, and these top campaigns are only a portion of the total scam robocalls made.² **In 2021, Tennesseans received nearly 1.8 billion robocalls (see Robocalls in Tennessee graph), almost 750 million (42%) of which were scam robocalls**—or between 11 and 12 scam robocalls for each Tennessean per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, more than 700,000 Tennesseans lost money to scam robocalls in 2021.⁵

1. Tennessee helps shut down fraudulent robo-call charity operation that took millions from people, WVLT 8 (Mar. 5, 2021).

2. YouMail confidential data provided to NCLC. We multiplied the number of calls from the top 1,000 scam robocall campaigns nationwide in January by Tennessee’s share of the US adult population (2.1%) to estimate calls made to Tennessee phones in January.

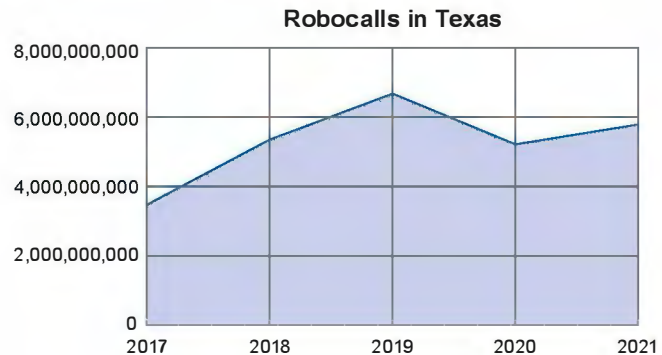
3. YouMail, “Historical Robocalls by State” (2022). YouMail, “U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index.” Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Tennessee and then calculated the number per adult Tennessean (see note 5) per month.

4. Roger Grimes, “Smishing 101 and Defenses,” KnowBe4 (Jan. 8, 2020).

5. TrueCaller, “TrueCaller Insights 2021 U.S. Spam & Scam Report” (2021). Truecaller’s survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Tennessee’s adult population (5,433,695 in 2021, per the U.S. Census Bureau) is 749,850.

Scam Robocalls in Texas

Eddie Gerinski of Austin receives robocalls almost every day. Not only that, but he also discovered that robocallers had been spoofing his number to victimize other Texans, once he started getting calls from confused people saying he had called them.¹



According to estimates based on data from YouMail, the most prevalent scam campaigns of January 2022 accounted for nearly 39 million scam robocalls made to Texas phones in that month alone, and these top campaigns are only a portion of the total scam robocalls made.² **In 2021, Texans received nearly 5.8 billion robocalls** (see Robocalls in Texas graph), **about 2.4 billion (42%) of which were scam robocalls**—or about 9 scam robocalls for each Texan per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, over 3 million Texans lost money to scam robocalls in 2021.⁵

1. Brad Streicher, “[Texans get millions of robocalls every day, per national data](#),” KVUE (May 14, 2021).

2. YouMail confidential data provided to NCLC. We multiplied the number of calls from the top 1,000 scam robocall campaigns nationwide in January by Texas’ share of the US adult population (8.5%) to estimate calls made to Texas phones in January.

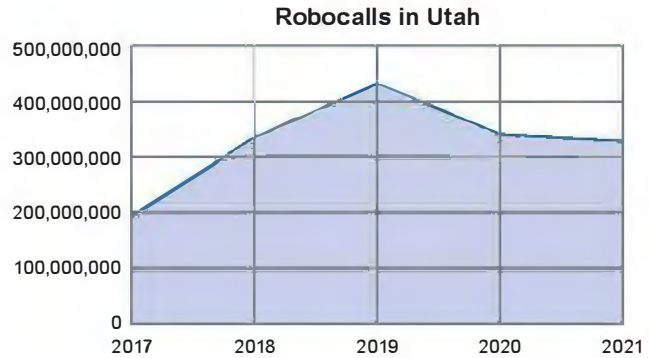
3. YouMail, “[Historical Robocalls by State](#)” (2022). YouMail, “[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#).” Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Texas and then calculated the number per adult Texan (see note 5) per month.

4. Roger Grimes, “[Smishing 101 and Defenses](#),” KnowBe4 (Jan. 8, 2020).

5. TrueCaller, “[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)” (2021). Truecaller’s survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Texas’ adult population (21,998,316 in 2021, per the [U.S. Census Bureau](#)) is 3,035,768.

Scam Robocalls in Utah

While taking care of her grandchildren, Machel, a Utah woman, received a robocall about a problem with her Social Security number. When she called back, a fake representative told her that her Social Security number had been “compromised” and was being used by a powerful drug cartel and that her family was in danger. She was told that to protect her money she needed to wire it to an offshore account. She wired more than \$150,000 to an account in Hong Kong before realizing it was a scam.¹



Sadly, Machel is far from the only Utahn to encounter this kind of robocall scam. According to estimates based on data from YouMail, nearly 78,000 scam Social Security robocalls were made to Utah phones in January 2022 alone.² **In 2021, Utahns received nearly 327 million robocalls (see Robocalls in Utah graph), about 137 million (42%) of which were scam robocalls**—or between 4 and 5 scam robocalls for each Utahn per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, well over a quarter million Utahns lost money to scam robocalls in 2021.⁵

1. Michael George, “[Robocall scam targeting senior citizens’ social security](#),” Central Illinois Proud (Feb. 1, 2020).

2. YouMail confidential data provided to NCLC, filtered by campaigns related to Social Security scams. We multiplied nationwide scam Social Security robocalls in January by Utah’s share of the US adult population (0.9%) to estimate calls made to Utah phones in January.

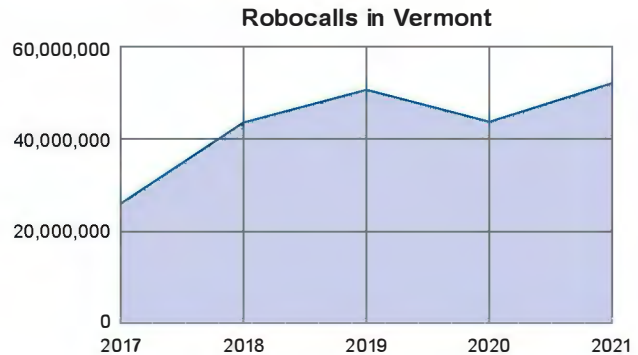
3. YouMail, “[Historical Robocalls by State](#)” (2022). YouMail, “[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#).” Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Utah and then calculated the number per adult Utahn (see note 5) per month.

4. Roger Grimes, “[Smishing 101 and Defenses](#),” KnowBe4 (Jan. 8, 2020).

5. TrueCaller, “[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)” (2021). Truecaller’s survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Utah’s adult population (2,369,962 in 2021, per the [U.S. Census Bureau](#)) is 327,055.

Scam Robocalls in Vermont

Vermont’s Attorney General reported earlier this year that the most common scam victimizing Vermont consumers was the “computer tech support” scam. In this scam, scammers claimed to be tech support workers, in order to gain access to consumers’ computers.¹



But these are not the only robocall scams targeting Vermonters. According to estimates based on data from YouMail, the most prevalent scam campaigns of January 2022 accounted for more than 900,000 scam robocalls made to Vermont phones in that month alone, and these top campaigns are only a portion of the total scam robocalls made.² **In 2021, Vermonters received more than 52 million robocalls** (see Robocalls in Vermont graph), **nearly 22 million (42%) of which were scam robocalls**—or between 3 and 4 scam robocalls for each Vermonter per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, over 72,000 Vermonters lost money to scam robocalls in 2021.⁵

1. VermontBiz, “[Top 10 scams of 2021 released by Vermont AG: Tech support number 1](#)” (Jan. 12, 2022).

2. YouMail confidential data provided to NCLC. We multiplied the number of calls from the top 1,000 scam robocall campaigns nationwide in January by Vermont’s share of the US adult population (0.2%) to estimate calls made to Vermont phones in January.

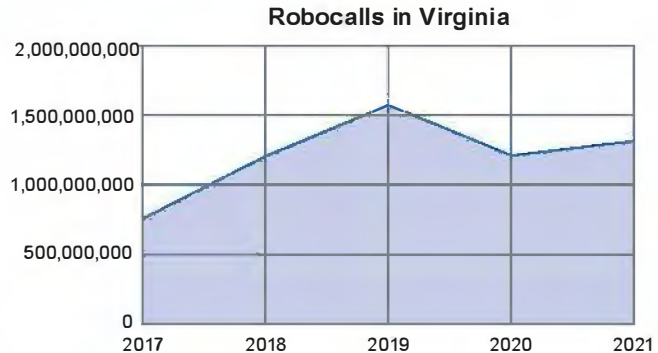
3. YouMail, “[Historical Robocalls by State](#)” (2022). YouMail, “[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#).” Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Vermont and then calculated the number per adult Vermonter (see note 5) per month.

4. Roger Grimes, “[Smishing 101 and Defenses](#),” KnowBe4 (Jan. 8, 2020).

5. TrueCaller, “[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)” (2021). Truecaller’s survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Vermont’s adult population (527,431 in 2021, per the [U.S. Census Bureau](#)) is 72,785.

Scam Robocalls in Virginia

June, a Virginia retiree who cares for her disabled son, received an automated voicemail last year ostensibly from the SSA about her Social Security number. When she returned the call, a fake “federal drug agent” threatened her with arrest for drug trafficking and told her that she was under investigation and had to surrender half the money in her bank accounts. She was forced to drive from bank to bank while on the phone with the scammer, withdrawing money and buying gift cards to send to him. The scam went on for weeks. June suffered bouts of insomnia and began receiving hundreds of other scam calls every week, forcing her to change her phone number 3 times in 9 months. She lost nearly all of her \$500,000 in savings, and now lives on her son’s disability payments and her Social Security.¹



Sadly, June is far from the only Virginian to encounter this kind of robocall scam. According to estimates based on data from YouMail, nearly 225,000 scam Social Security robocalls were made to Virginia phones in January 2022 alone.² **In 2021, Virginians received more than 1.3 billion robocalls** (see Robocalls in Virginia graph), **553 million (42%) of which were scam robocalls**—or between 6 and 7 scam robocalls for each Virginian per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, nearly a million Virginians like June lost money to scam robocalls in 2021.⁵

1. Frank Green, “[Chesterfield woman’s life is upended in \\$10 million robocall scam](#),” Richmond Times-Dispatch (June 10, 2021).

2. YouMail confidential data provided to NCLC, filtered by campaigns related to Social Security scams. We multiplied nationwide scam Social Security calls in January by Virginia’s share of the US adult population (2.6%) to estimate calls made to Virginia phones in January.

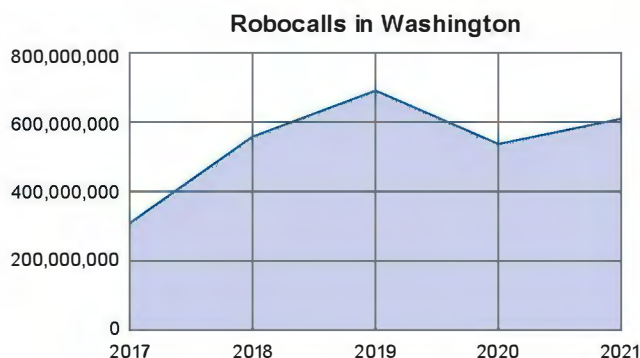
3. YouMail, “[Historical Robocalls by State](#)” (2022). YouMail, “[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#).” Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Virginia and then calculated the number per adult Virginian (see note 5) per month.

4. Roger Grimes, “[Smishing 101 and Defenses](#),” KnowBe4 (Jan. 8, 2020).

5. TrueCaller, “[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)” (2021). Truecaller’s survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of the adult population of Virginia (6,758,258 in 2021, per the [U.S. Census Bureau](#)) is 932,640.

Scam Robocalls in Washington

AARP reports on the top five scam robocall campaigns made to the Seattle/Tacoma/Bellevue area. On more than one occasion, its updates have included business impersonation scams, which prompt consumers to contact a false call-back number, typically about a purchase the consumer never made or a problem with the consumer's account.¹



According to estimates based on data from YouMail, more than 448,000 business impersonation scam robocalls were made to Washington phones in January 2022 alone.² **In 2021, Washingtonians received more than 616 million robocalls** (see Robocalls in Washington graph), **nearly 260 million (42%) of which were scam robocalls**—or between 3 and 4 scam robocalls for each Washingtonian per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, over 835,000 Washingtonians lost money to scam robocalls in 2021.⁵

In March, Washington's Attorney General launched a new anti-robocall initiative, designed to combat harassing, fraudulent, and illegal robocalls. Washington consumers can now report robocalls they have received to the state's [Robocall Complaint Form](#).⁶

1. [Tip-Offs to Rip-Offs: Top five robocall scams in Seattle/Tacoma/Bellevue](#), AARP (updated Apr. 11, 2022).

2. YouMail confidential data provided to NCLC. We multiplied the number of calls from the top 1,000 scam robocall campaigns nationwide in January by Washington's share of the US adult population (2.3%) to estimate calls made to Washington phones in January.

3. YouMail, "[Historical Robocalls by State](#)" (2022). YouMail, "[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#)." Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Washington and then calculated the number per adult Washingtonian (see note 5) per month.

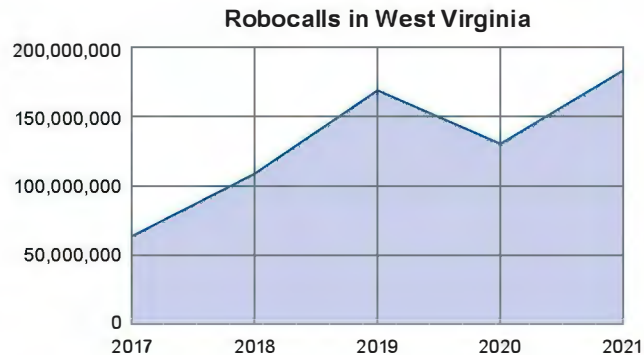
4. Roger Grimes, "[Smishing 101 and Defenses](#)," KnowBe4 (Jan. 8, 2020).

5. TrueCaller, "[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)" (2021). Truecaller's survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Washington's adult population (6,051,657 in 2021, per the [U.S. Census Bureau](#)) is 835,129.

6. Washington State Office of the Attorney General, "[AG Ferguson launches anti-robocall initiative to stop illegal, harassing calls](#)" (March 29, 2022).

Scam Robocalls in West Virginia

West Virginia’s Attorney General last year urged consumers to be wary of scam robocalls that falsely claim “fraudulent activity” has been detected in a consumer’s account. The scammer uses the fake “alert” to gain the consumer’s account information and steal money.¹



Unfortunately, this kind of robocall scam is not rare. According to estimates based on data from YouMail, more than 84,000 scam “fraud alert” robocalls were made to West Virginia phones in January 2022 alone.² **In 2021, West Virginians received more than 180 million robocalls (see Robocalls in West Virginia graph), nearly 77 million (42%) of which were scam robocalls**—or between 4 and 5 scam robocalls for each West Virginian per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, nearly 200,000 West Virginians lost money to scam robocalls in 2021.⁵

1. Jonathan Weaver, “[West Virginia attorney general warns of fraudulent activity scam](#),” WVNews (April 15, 2021).

2. YouMail confidential data provided to NCLC, filtered by campaigns related to fraud alerts. We multiplied nationwide scam fraud alert robocalls in January by West Virginia’s share of the US adult population (0.6%) to estimate calls made to West Virginia phones in January.

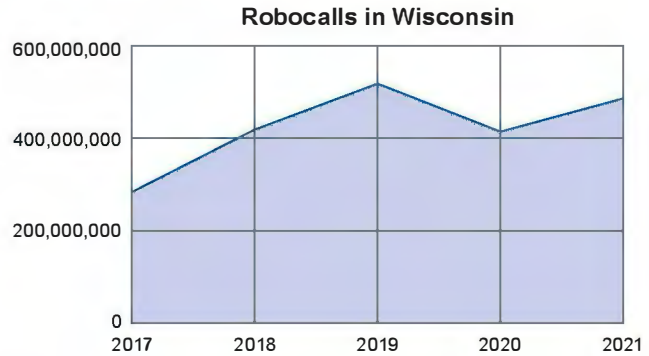
3. YouMail, “[Historical Robocalls by State](#)” (2022). YouMail, “[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#).” Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in West Virginia and then calculated the number per adult West Virginian (see note 5) per month.

4. Roger Grimes, “[Smishing 101 and Defenses](#),” KnowBe4 (Jan. 8, 2020).

5. TrueCaller, “[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)” (2021). Truecaller’s survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of West Virginia’s adult population (1,424,584 in 2021, per the [U.S. Census Bureau](#)) is 196,593.

Scam Robocalls in Wisconsin

According to Wisconsin's Department of Agriculture, Trade & Consumer Protection, the number one phone scam reported by Wisconsin consumers is the utility scam. Scammers claim that the consumer's utilities will be disconnected unless an immediate payment is made.¹



According to estimates based on data from YouMail, nearly 100,000 scam “utilities” robocalls were made to Wisconsin phones in January 2022 alone.² **In 2021, Wisconsinites received nearly 500 million robocalls** (see Robocalls in Wisconsin graph), **about 200 million (42%) of which were scam robocalls**—or between 3 and 4 scam robocalls for each Wisconsinite per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, well over half a million Wisconsinites lost money to scam robocalls in 2021.⁵

1. Tammy Elliott, “Consumer alert: Robocalls, scam calls hit record high,” WEAU 13 News (Feb. 21, 2021).

2. YouMail confidential data provided to NCLC, filtered by campaigns related to utilities bills. We multiplied nationwide scam utilities robocalls in January by Wisconsin’s share of the US adult population (1.8%) to estimate calls made to Wisconsin phones in January.

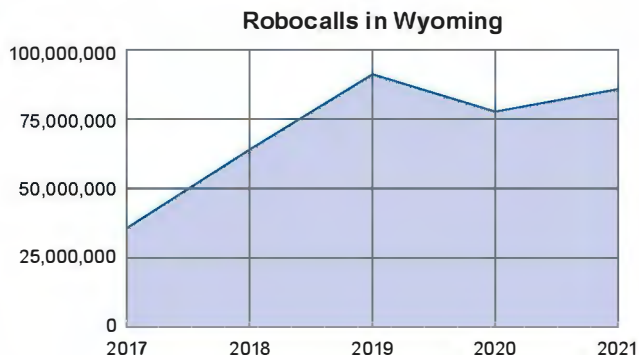
3. YouMail, “Historical Robocalls by State” (2022). YouMail, “U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index.” Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Wisconsin and then calculated the number per adult Wisconsinite (see note 5) per month.

4. Roger Grimes, “Smishing 101 and Defenses,” KnowBe4 (Jan. 8, 2020).

5. TrueCaller, “TrueCaller Insights 2021 U.S. Spam & Scam Report” (2021). Truecaller’s survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Wisconsin’s adult population (4,610,600 in 2021, per the U.S. Census Bureau) is 636,263.

Scam Robocalls in Wyoming

According to Wyoming’s Health Department, scammers are using robocalls to target residents with fake healthcare related calls. Scammers ask for consumers’ personal insurance and financial information and spoof their phone numbers so that the calls appear to come from the state.¹



This scam is far from rare.

According to estimates based on data from YouMail, more than 140,000 scam “health insurance” robocalls were made to Wyoming phones in January 2022 alone.² **In 2021, Wyomingites received more than 85 million robocalls (see Robocalls in Wyoming graph), nearly 36 million (42%) of which were scam robocalls**—or between 6 and 7 scam robocalls for each Wyomingite per month.³ And calls are not the only scams consumers must deal with: scam text messages are on the rise too.⁴

These robocalls have a cost. According to estimates based on TrueCaller survey data, over 60,000 Wyomingites lost money to scam robocalls in 2021.⁵

1. Associated Press, “[Phone scammers take advantage of Wyoming information breach](#),” U.S. News & World Report (April 30, 2021).

2. YouMail confidential data provided to NCLC, filtered by campaigns related to health insurance. We multiplied nationwide scam health insurance robocalls in January by Wyoming’s share of the US adult population (0.2%) to estimate calls made to Wyoming phones in January.

3. YouMail, “[Historical Robocalls by State](#)” (2022). YouMail, “[U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#).” Forty-two percent of all robocalls were scams, according to YouMail. We applied this percentage to the number of robocalls in Wyoming and then calculated the number per adult Wyomingite (see note 5) per month.

4. Roger Grimes, “[Smishing 101 and Defenses](#),” KnowBe4 (Jan. 8, 2020).

5. TrueCaller, “[TrueCaller Insights 2021 U.S. Spam & Scam Report](#)” (2021). Truecaller’s survey data indicates that 23% of Americans lost money to phone scams in 2021, and 60% of those who lost money lost it to robocall scams (13.8% of Americans). 13.8% of Wyoming’s adult population (445,100 in 2021, per the [U.S. Census Bureau](#)) is 61,424.

Methodology

Similar data points appear on each of the state pages featured in Appendix 2. We offer these estimates as a starting place for consumers and policymakers to develop a sense of the magnitude of the scam robocall problem in their state. We aim to provide more nuanced estimates and robust information in future publications, and welcome assistance from state and federal officials to achieve that goal.

The first paragraph on a page typically describes actual harm suffered by phone subscribers in that state due to scam robocalls, or describes recent efforts undertaken by state officials to reduce the harm from scam robocalls in that state. The first paragraph for some pages (e.g. Alabama) includes data that might otherwise appear in the second paragraph.

The second paragraph addresses multiple data points, coupled with Census data:

- Estimated scam robocalls of a particular type within that state in a month (e.g. IRS scams), using confidential scam robocall campaign data provided by YouMail; and
- Estimated scam robocalls within that state in a year, and per person per month, using public data provided by YouMail.

Confidential data on the Top 1,000 scam robocall campaigns in January 2022 was provided to NCLC by YouMail. The dataset provided was nationwide in scale, and not broken out by state. Some pages refer to a specific campaign (e.g. IRS scams), and some pages refer to the top 1,000 scam robocall campaigns broadly. As we note on each page (typically in footnote 2), we analogized, using what percentage of the total adult population of the U.S. lived in that state, as reported by the Census, to estimate what percentage of these top scam robocall campaigns were made to consumers within that state. This is an imperfect estimate, as it seems unlikely that scam robocalls are evenly distributed amongst phone subscribers across the United States.

Public data on annual scam robocalls made to each state in 2021 was taken from YouMail's [Robocall Index](#), then multiplied by 42%, the nationwide average of robocalls that were scam robocalls, as reported in a recent YouMail press release,¹ to derive the estimated scam robocalls to each state last year. Again, this is an imperfect estimate, as it seems unlikely that the percentage of robocalls that are scam robocalls is identical across each of the fifty states. To calculate the estimated scam robocalls per person per month, we divided the number of

1. YouMail, "U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index," PR NewsWire (Jan. 6, 2022).

estimated annual scam robocalls in that state by the adult population of that state, as reported by the Census, and by 12 (this is described in a footnote on each state's page, typically footnote 3).

The third paragraph couples Harris Poll survey data, as reported by TrueCaller, with Census data, to estimate the number of consumers in that state who lost money to robocalls in 2021. This calculation is described in greater detail in a footnote on each state's page (typically footnote 5). Again, this is an imperfect estimate, as it seems unlikely that the percentage of adults who suffered financial losses due to scam robocalls is identical across the United States.



**National
Consumer Law
Center**

epic.org

**ELECTRONIC
PRIVACY
INFORMATION
CENTER**

NATIONAL HEADQUARTERS

7 Winthrop Square, Boston, MA 02110
(617) 542-8010

NCLC.ORG

WASHINGTON OFFICE

Spanogle Institute for Consumer Advocacy
1001 Connecticut Ave, NW, Suite 510
Washington, DC, 20036
(202) 452-6252



TUESDAY, APRIL 26, 2022

COMMUNICATIONS DAILY SPECIAL REPORT

Special Report on Robocall Scourge

The Robocall Scourge: Special Report Finds a Continuing Problem	1
Spoofing a Major Source of Callers' FCC Complaint Ire	2
States, Congress Fight Robocall 'Arms Race'	4
Political Robocalls Here to Stay Despite Effect on Voter Participation, Misinformation: Experts	6
A Year After SCOTUS' Duguid Decision, Companies Still Face TCPA Lawsuits	8
Robocalls a Problem in Other Countries, but Scams May Be Worse	10

The Robocall Scourge: Special Report Finds a Continuing Problem

Communications Daily presents our Special Report on efforts to confront the perennial problem of robocalls and robotexts, still the most common complaint received by the FCC. We look at efforts at the state, national and international levels to address a problem that many feel is only worsening, with spoofing and alluring links in robotexts now increasingly the methods of choice.

Leading us off, Comm Daily reporter Matt Daneman takes a close look at FCC data obtained in a Freedom of Information Act request, and concludes that spoofing is a particularly frequent subject of citizen complaints to the agency. He looks at a typical month of robocall complaints, which remain by far the most common ones the FCC receives.

State and federal legislators, acting together and independently, are working to address constituent rage over robocalls and robotexts, reports *Comm Daily's* states reporter Adam Bender. His story provides an overview of their efforts as elected officials seek to respond to this hottest of hot button issues.

Americans received about 852 million political robocalls and 18.5 billion political robotexts in 2020, according one count, reports *Comm Daily's* wireline reporter Gabriella Novello, and the trend will continue since political communications aren't banned by the Telephone Consumer Protection Act. She considers the effect on voters of calls that all too often use misinformation to discourage voting.

The definition of "automatic telephone dialing system" as reflected in the year-old *Facebook v. Duguid* Supreme Court decision is the focus of a report by *Comm Daily's* Howard Buskirk. The ruling reduced the number of Telephone Consumer Protection Act lawsuits and hasn't increased robocalls, as some predicted.

Comm Daily's European correspondent Dugie Standeford provides a look at efforts there to combat the robotext and robocall affliction. She reports that U.K. regulators in particular are responding to frequent complaints, which increasingly are about scams rather than mere annoyance.

[Share Article](#)

Complaints 'Often Critical' in Probes

Spoofing a Major Source of Callers' FCC Complaint Ire

Spoofing remains a particularly acute problem for U.S. residents already besieged by run-of-the-mill robocalls, with close to one in four robocall complaints to the FCC involving some form of spoofing, per our analysis of those complaints. The agency often says robocalls are the biggest source of public complaints it receives. Via a Freedom of Information Act request, we obtained and then reviewed the 446 complaints the agency received on one day, July 1. Per data from the agency's Consumer Complaints Center, it received just shy of 161,000 robocall complaints last year.

Those complaints are "often a critical part of investigations and sometimes prompt investigations" into robocallers, the FCC told us.

About 26% of the calls we analyzed came from either spoofed numbers or people saying their number was being fraudulently used for robocalls. "I just received a phone call and threat via text by someone who believes it was me who called them, when it wasn't," said a Chicago complaint. "Today I received a call from my own phone. I did not answer," per a Brooklyn Center, Minnesota, complaint. "My cellular phone number is continuously spoofed and I have had some very angry people call me back," said an Angelus Oaks, California, complaint.

A variety of those complaints show sizable amounts of incoming calls. A Houston, Tennessee, complainant reported 25-plus spam calls a day. A Quartz Hill, California, complainant told of elderly grandparents receiving 15-20 unwanted calls a day, and having blocked 30 numbers through their phone carrier "and still their phone rings off the hook with unwanted calls." A Siletz, Oregon, complainant reported receiving 20-30 unwanted texts a day: "I've blocked too many numbers to keep count. If I absolutely have no other choice than to change my number I guess I will it's just going to cause a lot of issues in my work and personal life ... I know there is a national do not call number for telemarketers is there one for text fishing?!?! If so I want on it please!!"

The complaints themselves vary widely, from including the number that had called and details about the calls to vague grouching about unwanted calls. Per our analysis, about 10% of calls involved vehicle warranty sales pitches. Auto warranty robocalls often are the top unwanted call complaint made to the FCC, the agency said. People in our analysis also made close to two dozen complaints about calls purportedly about IRS or Social Security problems.

Many complaints also urge FCC action. "IDENTIFY AND BLOCK THESE ROBOCALLER OFFENDERS!" said a Montrose, Colorado, complainant. "These repeat offenders repeatedly violate the No Call List and need to be identified, blocked, arrested and prosecuted! They are lawbreakers that solely exist to steal information or fraudulently [sic] swindle money." "WHY CAN'T THE FCC STOP THESE ABUSIVE PRACTICES," echoed an Eastchester, New York, complainant who received at least half a dozen unwanted faxes. The complainant said whoever answered the phone number listed on the fax was abusive and refused to cease sending them. A Cumming, Georgia, complainant—citing 10 calls in a month from the same number, all ending in hang-ups—said the person responsible "needs to be held accountable and their privilege of phone use taken away."

While their numbers differ, some telecom services companies see robocall volumes rebounding after a 2020 dip.

About 20% to 25% of all phone calls are robocalls, robocall blocking service YouMail blogged this month. “No wonder people are ... not bothering to answer their phone any more,” it said. There were an average of 13.3 robocalls per person in March, with 4.4 billion calls placed nationwide, said YouMail. It said robocall volume in 2021, at 50.5 billion, was up about 10% from 2020, though both years were down from 2019. Transaction Network Services’ robocall report last month said Americans were hit with 78.9 billion robocalls last year, up 2% from 2020 but down 26% from 2019. It said 61% of that volume originated via VoIP calls, and few originate on U.S. wireless networks. It said with implementation of the Stir/Shaken protocols improving call authentication across networks, robotexts are gaining in popularity with spammers as a route around the protocols. It said 48% of December robotext scams were from a robocall spammer.

Agency Action

The FCC said all its robocall and spoofing investigations involve the use of consumer complaints, “whether as the direct heart of the case or as supporting material that prompts a deeper dig into additional facts.” It said the \$225 million Rising Eagle spoofing fine (see 2103170061) “relied in part on consumer complaints,” with that investigation partially prompted by increasing health insurance telemarketing complaints in 2018. The FCC said consumer interviews confirmed the calls caused notable consumer harm, and Rising Eagle didn’t have consent to make the calls. It said the agency’s \$9.9 million spoofing fine, now the subject of DOJ litigation seeking collection (see 2110210048), “also started largely based on consumer complaints” to the FCC, FTC and local law enforcement.

Data from unwanted call complaints received at the FCC’s Consumer Complaint Center gets shared internally with other agency bureaus and offices “to inform policy and potential enforcement,” the commission said. That data gets analyzed for trending issues and to help inform consumer educational material such as scam alerts and consumer guides. Chairwoman Jessica Rosenworcel created the Robocall Response Team “in an effort to strengthen the relationships among Bureaus and Offices in the effort to address illegal robocalls,” said the FCC. The Enforcement Bureau often begins investigations based on information such as media reports of possible illegal spoofing campaigns or signs of malicious robocall campaigns brought to its attention by USTelecom’s Industry Traceback Group. Consumer complaints to their service providers or to call-blocking apps are used as ITG evidence to conduct private-led tracebacks of suspected illegal calls,

		EDITORIAL & BUSINESS HEADQUARTERS 2115 Ward Court, N.W., Washington, DC 20037		Business	
(ISSN 0277-0679) PUBLISHED BY WARREN COMMUNICATIONS NEWS, INC.		Albert Warren Editor & Publisher 1961–2006		Sheran Fernando Chief Operating Officer Brig Easley Exec. VP-Controller Gregory E. Jones Director of IT Services Annette Munroe Director of Operations Katrina McCray Office Manager Loraine Taylor Administrative Assistant	
Timothy Warren Executive Managing Editor		Paul Warren Chairman and Publisher Daniel Warren President and Editor Timothy Warren Executive Managing Editor Paul Gluckman Executive Senior Editor Howard Buskirk Executive Senior Editor Rebecca Day Senior Editor Matt Daneman Senior Editor Adam Bender Senior Editor Monty Tayloe Associate Editor Jimm Phillips Associate Editor Karl Herchenroeder Associate Editor Gabriella Novello Assistant Editor Debra Rubin News Editor		Sales	
Warren Communications News, Inc. is publisher of Communications Daily, Consumer Electronics Daily, International Trade Today, Export Compliance Daily, Trade Law Daily and other specialized publications.		Michael Feazel Consulting Editor		William R. Benton Sales Director Bruce Ryan Account Manager Jim Sharp Account Manager Lisa Price Account Manager Matt Long Account Manager Matt Peterson Account Manager Walt Sierer Account Manager	
Send news materials to newsroom@warren-news.com		International Trade Today		Phone: 202-872-9200 Fax: 202-318-8984 https://warren-news.com Email: info@warren-news.com	
Follow <i>Communications Daily</i> on Twitter: https://twitter.com/Comm_Daily		Tim Warren Executive Managing Editor Brian Feito Managing Editor Mara Lee Associate Editor Ian Cohen Associate Editor Jacob Kopnik Associate Editor Ben Perkins Assistant Editor		Advertising Sales Representation by Richard Nordin, Group Nordin Phone: 703-819-7976 Fax: 202-478-5135 richard@groupnordin.com	
Follow Warren Communications News on Facebook: https://www.facebook.com/WarrenCommunicationsNews		Copyright © 2022 by Warren Communications News, Inc. Recipients may copy and share this report provided that information on Warren is not removed.			

with the bureau using those investigations' findings "as evidence in its cease and desist letters to bad actor voice service providers," the FCC said.

Consumer complaints might be used by the Enforcement Bureau and agency leadership to inform decisions about the harms triggered by a particular calling campaign, with the result being "upward adjustments for egregiousness in proposed fines as allowed under the law to reflect harmful impacts," the FCC said. It said it also has taken different consumer protection initiatives informed by consumer complaints, including focusing on one-ring scams, enabling voice providers to block illegal calls before they reach consumers' phones and requiring that Caller ID be authenticated to address spoofing scams. — *Matt Daneman*

[Share Article](#)

More Bills Coming

States, Congress Fight Robocall 'Arms Race'

Federal and state lawmakers are looking for new ways to tighten robocall restrictions amid an evolving landscape, but experts told us it's still challenging for governments to keep ahead of bad actors. Some on Capitol Hill are hoping to quickly enact a new anti-robocall package this year, despite a rapidly closing legislative window. State legislators are acting in case federal legislation stalls. Robocall opponents must "press on every front," said North Carolina Attorney General Josh Stein (D) in an interview: He believes stopping bad actors requires state and federal collaboration, and should include industry and other countries.

Stein believes states should continue to play a leading role due to their success in recent years. He cited his leadership of a bipartisan 51-AG coalition that worked with big telcos in 2019 to develop [anti-robocall principles](#) as "one of the most meaningful" efforts to curb bad actors in recent years. The principles focused on deploying technology to counter robocalls and improving telcos' cooperation with law enforcement. "We've actually seen some improvements," Stein said. He noted state AGs also pushed the FCC to do more, including a successful effort to shorten the deadline for small voice service providers that aren't facilities-based to implement Stir/Shaken (see [2112140023](#)).

"The next wave of enforcement" for state AGs is to hold accountable the "smaller phone companies that are making money off of robocalls" when they come through their networks, Stein said. "They have an actual financial incentive to turn a blind eye to the traffic." North Carolina sued gateway provider Articul8 on suspected fraudulent robocalls in January (see [2201250052](#)). Some AGs are expanding focus to automated text messages. Florida AG Ashley Moody (R) [said](#) Dec. 27 that robotexts are "now more prevalent, and potentially more dangerous, than robocalls since malicious links can be clicked on directly in a text."

Top lawmakers on the House and Senate Commerce committees are, meanwhile, eyeing how to translate FCC Chairwoman Jessica Rosenworcel's recent call for new bills to strengthen the commission's anti-robocall enforcement power into legislative language. Rosenworcel urged the House Communications Subcommittee in late March (see [2203310060](#)) to bypass DOJ and give the FCC direct authority to seek fines against robocallers in federal court. She has been [pressing](#) Congress for a fulsome update to the FCC authority, given the Supreme Court's narrowed definition of what constitutes an automatic telephone dialing system in *Facebook v. Duguid* (see [2104010063](#)).

Rep. Anna Eshoo, D-Calif., told us she intends to follow through quickly on her promise at the House Communications hearing to work with Rosenworcel on legislation aimed at increasing the FCC's robocall enforcement authority. "I would hope we can move quickly" on such a bill because "there isn't anyone in this country who can stand up and say 'I love robocalls,'" Eshoo said: "When something doesn't

work well, you need to fix it.” It’s clear “DOJ is not going after these spammers” with sufficient force, so “the FCC should have the authority,” she said.

Sen. Ed Markey, D-Mass., is also interested in pursuing legislation to increase the FCC’s robocall enforcement authority in the ways Rosenworcel proposes, he told us. “It’s a crisis that continues” to require Congress’ attention, he said. A Markey aide later said he aims for future legislation to “build on” what Congress included in the 2019 Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (Traced) Act (see [1912310028](#)), including via the Robocall Trace Back Enhancement Act. [S-3335](#) would protect the Traced Act’s USTelecom-led Industry Traceback Group by providing immunity from lawsuits for “receiving, sharing and publishing” certain “covered” trace back information, including information related to “suspected fraudulent, abusive or unlawful robocalls” (see [2112080059](#)).

Senate Communications Subcommittee ranking member John Thune, R-S.D., believes Rosenworcel’s request for more direct FCC enforcement authority is “a fair request” since robocalls remain a problem nationwide. “We’d be happy to look at adding some additional clarity and direction to the authority” the FCC already has, the Traced Act lead sponsor told us: “There’s got to be a consequence to these folks who perpetuate these schemes in the first place” and Congress should consider reworking the current FCC-DOJ arrangement if it’s “not sufficient.” The Traced Act is a relatively new statute, but “the bad guys always come up with new ways of getting around” the law and further legislation may be needed to catch up, Thune said.

“We’re getting short on time” to enact robocall legislation in this Congress, but doing more to address the issue is “clearly a priority for the American people,” said House Communications Subcommittee ranking member Bob Latta, R-Ohio. “People are still being overwhelmed by this stuff” and if current statutes “aren’t working” fully, then “we’ve got to do something else to stop” the calls.

“There’s not a lot of time left” this session for lawmakers to get a package through given the looming start of amplified campaigning ahead of the November midterm elections, said National Consumer Law Center Senior Counsel Margot Saunders. “Anything that goes through would probably have to move via unanimous consent in the Senate, which would mean that it could pass, but on the other hand how effective might it be?” There’s “a lot of sentiment in support of doing something,” but it’s still unclear whether any proposal would get bipartisan support, she said.

Rosenworcel’s bid for enhanced FCC enforcement authority will carry significant weight, but stakeholders are floating a range of other ideas behind the scenes, Saunders said. One proposal that could “gain traction” as part of a consensus package involves “taking the Do Not Call registry and updating it considerably,” including “allowing subscribers to identify what types of automated calls they want to allow without consent.”

Advocates stopped seriously pushing for legislation to expand the narrowed autodialer definition the Supreme Court created in *Facebook*, which Markey and Eshoo explored in the ruling’s immediate aftermath. NCLC “spent quite a bit of time investigating” the potential for a legislative fix for the ruling and “essentially gave up” on that, Saunders said: “There’s too many people on our own side” who backed the top court’s decision, so “we saw it as a nonstarter. We can draft legislation. We can get it introduced. We might even get it heard at a committee meeting. But it’s not going to pass.”

'Popular' but 'Tricky' Fight

Fighting robocalls is a “very popular” for state legislators of both political parties, said Heather Morton, program principal-fiscal affairs, National Conference of State Legislatures. She sent a [list](#) of about 80 state bills this year on unsolicited communications. State bills tend to propose increasing penalties for

violations or incorporating federal requirements, like following Stir/Shaken protocols, in state law, Morton said: Some aim to specifically protect vulnerable communities like seniors. However, as soon as states pass new laws, “bad actors figure out ways to get around them,” said Morton. “The issue’s not going away. More bills will be coming.”

South Dakota enacted an anti-robocalls bill last month. Other measures advanced recently in states including Hawaii and Oklahoma (see [2203170023](#)) and [2204070027](#)). New York Gov. Kathy Hochul (D) signed anti-robocall bills in November to require telecom companies to block certain numbers and implement Stir/Shaken protocols to validate calls (see [2111080019](#)).

Illinois Senate Commerce Committee Chair Suzy Glowiak Hilton (D) said caller-ID spoofing came to her attention when she and her neighbors kept getting calls that appeared to come from people or businesses they trusted, she said in an interview. Glowiak Hilton is especially concerned about vulnerable seniors, she said. Her bill ([SB-2225](#)) to ban spoofing passed the Senate with no opposition last year but hasn’t budged in the House. Enforcement is the “tricky part” with stopping spoofed calls, Glowiak Hilton said. “It’s hard to catch anybody doing it,” and there’s often no financial loss associated with someone receiving an annoying call. With limits to state authority, the federal government must also “step up,” she said.

It’s not “an easy problem to fix,” agreed Illinois Assembly Commerce Committee Chairman Marcus Evans (D). He introduced [HB-4598](#) in January to make caller-ID spoofing a misdemeanor offense. One challenge is not casting the net so wide as to capture cold calling by legitimate businesses, Evans said. His bill might not be the “clear-cut solution,” he said, but he believes proposing state laws is important to raising awareness and prioritizing the issue.

State AGs continue to show wide bipartisan interest in stopping robocalls through enforcement actions and pushing the FCC, said Crowell attorney Clayton Friedman. AGs tend to “up the gas” when federal action slows, but even with the Biden administration increasing focus, state enforcers aren’t letting up, he said. State law enforcement faces jurisdictional barriers, said the lawyer: “The frustration that they see is so many [calls] are coming from overseas.”

“It is regularly the top complaint that my office receives year in and year out,” said North Carolina AG Stein. His office [reported](#) receiving 10,011 consumer complaints about telemarketing and robocalls in 2021, out of 28,043 total complaints that year. Stein isn’t alone: Robocalls and “bogus telemarketing” made top-complaint lists for many states last year, [said](#) the National Attorneys General Training and Research Institute.

The challenge is that robocallers are “making billions of dollars committing fraud on vulnerable people,” said Stein. “Every time either the regulators or the phone companies ... make an advance in our fight against robocallers, they’re going to come up with some counter to go around that because the financial incentives are so great,” said the AG: It’s an “arms race” that will take time to win.

Our interview with Stein was interrupted by a call to him from Palisade, Colorado. He said Verizon flagged it as potential spam. — *Adam Bender and Jimm Phillips*

[Share Article](#)

More Robotexts?

Political Robocalls Here to Stay Despite Effect on Voter Participation, Misinformation: Experts

Political campaign-related robocalls and robotexts may have a negative effect on voter participation and are likely to continue for the foreseeable future, telecom and election experts told us. Voters received

an unprecedented number of robocalls and robotexts leading up to the 2020 presidential election, and many sought FCC action to curb those that are unwanted and potentially illegal, according to consumer complaints we analyzed (see [2011030050](#)).

Political robocalls made to cellphones are prohibited without the called party's prior express consent under the Telephone Consumer Protection Act. Political robocalls aren't prohibited when made to a landline phone without consent. Americans received about 852 million political robocalls and 18.5 billion political robotexts in 2020, according TelTech's RoboKiller. The company estimated consumers received nearly 94 million robocalls and more than 2 billion text messages in November 2020 related to the presidential election.

The number of robocalls and robotexts sent during the 2020 election cycle reached "record levels," said Giulia Porter, RoboKiller vice president-marketing, in part because much of the technology behind political texting "really wasn't around as much and as prominently" in earlier cycles. Most robocalls the company saw were sent with prerecorded messages, Porter said.

In the week leading up to the 2020 presidential election, the FCC received more than 500 consumer complaints, according to documents we obtained and reviewed through a Freedom of Information Act request. One New York consumer complained about receiving a prerecorded call from an unidentified person and hadn't given consent. An Ohio consumer reported receiving a prerecorded call from a blocked caller despite being on the National Do Not Call Registry. Porter said RoboKiller received user feedback during the election cycle about people unsubscribing from a robocaller but continuing to receive calls.

An FCC spokesperson said Chairwoman Jessica Rosenworcel "supports robust citizen participation," but the FCC "does not target political calls specifically." If robocalls "happen to be political in nature and violate our robocall or spoofing rules, those rules would be applied in our enforcement actions, regardless of the nature of the call," he said. All prerecorded voice message calls, campaign-related and otherwise, must clearly state at the beginning of the prerecorded message the identity of the individual or entity initiating the call. They must also provide the telephone number of the calling party either during or after the message.

Some political calls and texts consumers complained to the FCC about during the 2020 election cycle probably weren't made with an autodialer, and therefore don't require prior express consent, said Mac Murray & Shuster's Michele Shuster: "It's perfectly legal to make telephone calls if you don't use a prerecorded message or an automatic telephone dialing system (ATDS)" (see [2204220042](#)).

If a consumer received a robocall or text that's governed by TCPA, it may be because the consumer gave consent when signing up for messages from another organization that may have listed entities it would share data with on its consent form, Shuster said. It "happens all the time," she said, but organizations can transfer lists of phone numbers without having prior consent if calls aren't being made using ATDS.

Although most consumers reported unsolicited robocalls from political candidates or organizations about the 2020 election, many said they also received unwanted robotexts. One Arkansas consumer reported receiving 22 texts from a political party despite asking for them to stop. A North Carolina consumer said texts about whether and how they voted were "an extreme invasion of privac[y]."

Robotexts are treated as calls under TCPA and subject to the same prohibitions as robocalls to wireless phones. Rosenworcel circulated an NPRM in October that "proposed requiring mobile wireless providers to block illegal text messaging" and "update commission policies to stop more unwanted robotexts," a spokesperson said, and she "hopes to see swift action from her colleagues on this item." An aide told us it's likely the item will move slowly.

The severity of robocalls and robotexts' impact on voter intimidation is “prevalent in the ecosystem,” said David Brody, Lawyers' Committee for Civil Rights Under Law managing attorney-digital justice initiative, but it's “extremely difficult to quantify.” The “one-on-one communication” of a robocall or robotext is also “invasive and impacting” because “it's difficult to trace and attribute the call,” he said.

Intimidating robocalls and robotexts about elections or voting are usually sent anonymously or “in a way where it's really difficult to figure out where it came from,” Brody said. It's difficult to “identify people who received the call and who were injured by it,” he said, and these kinds of robocalls make it more difficult for the “legitimate stuff to get the attention it deserves.” Robotexts including misinformation during the 2020 election were “highly targeted” to specific people and states or regions, Porter said.

Legal Action

The FCC has taken some action on suspected illegal political campaign-related robocalls in recent years. The Telephone Consumer Protection Act gives the FCC authority to issue a notice of apparent liability without issuing a citation first, and it did so in 2021 against John Burkman and Jacob Wohl for making 1,141 unlawful prerecorded calls to wireless phone numbers without prior express consent (see [2108240082](#)). The commission proposed a \$5 million fine after an Enforcement Bureau investigation found Burkman and Wohl sent prerecorded messages to potential voters that said their personal information would be used by law enforcement and credit card companies if they voted by mail.

The Lawyers' Committee filed a lawsuit against Burkman and Wohl in October 2020 under the Voting Rights Act and Ku Klux Klan Act. A U.S. District Court for the Southern District of New York granted the group a temporary restraining order that prohibited the two men from sending any additional robocalls or robotexts without written express consent throughout the rest of the 2020 election.

“Because of the vastly greater population they can reach instantly with false and dreadful information, contemporary means of voter intimidation may be more detrimental to free elections than the approaches taken for that purpose in past eras,” wrote Judge Victor Marrero in his October 2020 order, calling Burkman and Wohl's actions “electoral terror using telephones, computers, and modern technology.” The case, no. [1:20-cv-08668](#), is ongoing, as the Lawyers' Committee and National Coalition on Black Civic Participation are in a discovery phase for more information about the robocall campaign.

Not all political calls and texts are harmful, Brody said, and can “be really good, useful ... information” about how to register to vote or where a person's polling place is. It's “worth considering ... the role that data brokers play in this,” he said. Not having a fully staffed FCC and FTC “significantly impairs their ability to take action on these problems,” Brody said, saying Congress should pass privacy legislation.

With the 2022 midterm election cycle underway, RoboKiller is watching to see whether the use of political texts will continue to grow in the same direction as it did in 2020, Porter said. If it does, that may indicate that the trend “is here to stay for the foreseeable future, and probably ... for the next presidential election,” she said. — *Gabriella Novello*

[Share Article](#)

'Mini-TCPAs'

A Year After SCOTUS' Duguid Decision, Companies Still Face TCPA Lawsuits

In the aftermath of the Supreme Court's decision a year ago in *Facebook v. Duguid*, Telephone Consumer Protection Act lawsuits continue to be filed, lawyers told us, though at a lower rate than before the court acted. A year ago, a unanimous court sided with Facebook (see [2104010063](#)), favoring a narrow

definition of what constitutes an automatic telephone dialing system (ATDS). Lawyers also warned that some states, led by Florida, are engaging and that some litigation is shifting to the states.

Since the *Duguid* case was decided, a number of plaintiffs have brought cases based on footnote 7 in the Facebook opinion, which suggests “an autodialer might use a random number generator to determine the order in which to pick phone numbers from a preproduced list,” lawyers said. Plaintiffs argue that equipment “that uses a random or sequential number generator to determine the order in which to dial phone numbers from a preproduced list constitutes an ATDS,” said law firm McGuireWoods in a [note](#) to clients.

“The Supreme Court’s unanimous decision in *Duguid* provided clear direction to callers, courts, the FCC and litigants about the correct interpretation” of ATDS, said Hogan Lovells’ Mark Brennan: “Despite the pitched rhetoric by some that the court’s decision would lead to more robocalls, it has not. This underscores what legitimate callers have been saying all along, the robocall problem is being driven by fraudsters and scammers who aren’t following the TCPA regardless of how you interpret ATDS.”

TCPA cases aren’t going away, Brennan said. “Post-*Duguid*, we’ve seen a meaningful drop in TCPA litigation filings, though the plaintiffs’ bar remains active in this space,” he said. “We’ve also seen increased activity at the state level, with more ‘mini-TCPAs’ starting to appear,” he said.

“There was not the immediate fall off of ATDS allegations and cases I was hoping would come, because the Supreme Court opinion was very clear,” said Kelley Drye’s Becca Wahlquist. Wahlquist said she has followed all the decisions since the *Duguid* ruling. “There are still ATDS cases pending out there, lots of them, as many circuit courts haven’t yet weighed in, and some district court decisions have allowed ATDS claims to move forward,” she said.

For the first months after the *Duguid* decision, district courts “were kind of reluctant to recognize how sweeping that ruling was, so they weren’t dismissing cases out of hand,” Wahlquist said: “Then there was this big movement where a ton of district courts started saying, ‘You know, the allegations you’re making in your complaint are about targeted calls to customers and you are a customer of this company, so that just isn’t going to be an ATDS. It’s not a randomly and sequentially generated number if a company is calling you at the number you gave them.’”

Wahlquist said in the most recent decision of note, the 8th U.S. Circuit Court of Appeals rejected a footnote 7 argument last month in *Beal v. Truman Road*, as did the 9th Circuit in an unpublished decision. In *Beal*, a bar was using customer-provided numbers, shuffling them using software and sending the customers texts saying they had won a free drink, she said. Plaintiffs claimed the bar was randomly generating numbers to call, she said. “The 8th Circuit was really firm” and said because the numbers were provided by customers they weren’t generated by ATDS, she said. The [decision](#) “was a big deal,” she said. “That’s the first circuit case decision after Facebook, interpreting Facebook,” she said.

Some action has moved to the states, led by Florida, Wahlquist said. She predicted more cases will be filed in state courts.

“The new revisions to the Florida Telemarketing Act and the Florida Do Not Call Act provide robust protection to consumers from unwanted communications,” [said](#) Florida-based law firm Jimerson Birr: “It also forces many businesses to revisit how they conduct their marketing and consumer communications. These changes should not be taken lightly. Florida businesses should conduct a thorough evaluation of their telemarketing policies and procedures to ensure compliance.”

“Most of the litigation has involved interpretations of a footnote in the *Duguid* opinion, that can be read to suggest that a system that randomly selects a number from a non-random list could be an ‘autodialer’ subject to the TCPA,” emailed Gus Hurwitz, professor at the University of Nebraska College of Law:

“Most courts seem to be rejecting that interpretation.” He said, “the real action on the robocall front has been, is, and will remain focused on implementation of STIR/SHAKEN.”

The FCC could provide more guidance on TCPA issues, but that’s unlikely under a split 2-2 commission, said Nelson Mullins’ Steven Augustino. He mentioned a recent [letter](#) Chairwoman Jessica Rosenworcel sent Rep. Vern Buchanan, R-Fla., that warned of diminished protection for consumers after the *Duguid* ruling.

“The chairwoman’s recent request to Congress to provide additional authority to address autodialers is an indication that there is not sufficient consensus to tackle the big TCPA issues right now,” Augustino said: “The principal attention appears to be focused on stopping scam calls and fraudulent robocalling schemes. Here there is unanimity in purpose and an urgent desire to stem the flow of such calls. I expect the FCC to take more aggressive enforcement, with increasing attention on those entities closest to the origination of the fraudulent calls.”

“In light of the Facebook case, the Chairwoman hopes Congress will act to clarify the definition of autodialers to help protect consumers against unwanted robocalls,” an FCC spokesperson emailed. — *Howard Buskirk*

[Share Article](#)

Global Cooperation Growing

Robocalls a Problem in Other Countries, but Scams May Be Worse

Unwanted marketing calls cause headaches worldwide, telecom and privacy regulators said. Robocalls have attracted so many complaints that in the past two years or so, the U.K. and Australia signed formal pacts with the U.S. to fight them. It appears, though, that scam calls may be becoming a far bigger concern.

The U.K. Office of Communications and the Information Commissioner’s Office jointly tackle nuisance and scam calls. The ICO leads on live and recorded marketing calls and nuisance text messages and emails, while Ofcom handles silent and abandoned calls, they [noted](#) in March 2021. The ICO received nearly 104,000 complaints about nuisance calls and text messages in 2020, a 20% decrease from the prior year that was due to the initial coronavirus lockdown. Over 2020, however, complaint numbers rose to a higher level than in the latter months of 2019, a 27% rise that Ofcom said it expected to continue into 2021. “A sharp rise in suspected scam text messages was also noted,” many of which tried to exploit the pandemic and the U.K.’s response to it.

The ICO regulates the Privacy and Electronic Communications Regulations, which give people specific rights with regard to e-communications, a spokesperson emailed: “There are specific rules on marketing calls, emails, texts, faxes, cookies, keeping communications secure and customer privacy.” The office publishes nuisance call [trends](#) broken down by month, contact type and call category of complaints. January had 5,646 total complaints: 3,303 live calls, 1,434 automated and 909 texts. February brought 5,683 total complaints, 3,445 live, 1,453 automated and 786 texts. The ICO also publishes its [enforcement actions](#). So far this year, it has fined about 12 companies for making unsolicited direct marketing calls. It hit one home improvement company with a 200,000 pound (\$261,000) fine in February.

The ICO and FTC agreed in a December 2020 [memorandum of understanding](#) to provide mutual legal assistance to enforce laws protecting personal information in the private sector, including on unsolicited commercial email and robocalls. They’re both members of the Unsolicited Communications Enforcement Network, which didn’t comment.

Ofcom has been working to reduce nuisance calls for years, and the problem is shifting to scams, it noted in a [proposal](#) for tackling scam calls. For one thing, it said, unwanted calls are now harder to de-

tect because callers are more likely to change their numbers often or to use a spoofed number. This means in many cases, the perpetrator is likely to have shifted to a new number by the time the problem has been reported, and it's harder to trace those making unwanted calls because the number hasn't been assigned to the person making the calls.

Australia is also active on robocalls. The Australian Communications and Media Authority responds to unwanted calls and messages by, for example, enforcing the Do Not Call Register Act 2006 and the Spam Act 2003, a spokesperson emailed. So far this year, ACMA has taken action against three companies for unwanted calls and texts, including a fine for spam marketing messages of over 3.7 million Australian dollars (\$2.7 million) against a sports betting firm. Last year it handled 14 telemarketing and spam investigations. ACMA signed a May 2021 mutual legal assistance MOU with the FCC to address unlawful automated or prerecorded voice message telephone calls, unsolicited texts and phone scams, and last month agreed to boost joint efforts with the Canadian Radio-television and Telecommunications Commission against unlawful telemarketing and spam.

However, “our complaint data indicates the single biggest area of concern about unsolicited communications is scams, making up between approximately 33% and 66% of complaints in any given year,” ACMA said. New rules it enacted are having “a real impact,” but “unfortunately, there is no silver bullet to stop scams.”

Germany outlaws calls for advertising purposes without prior express consent from the consumer, a spokesperson for telecom regulator BNetzA (Bundesnetzagentur) emailed. This applies to voice-to-voice and automated calls. The regulator prosecutes such unauthorized advertising calls and can impose fines of up to 300,000 euros (\$327,000). Consumers can withdraw consent at any time for no reason. Last year, BNetzA received more than 79,000 complaints about unauthorized phone advertising (calls without consent), the vast majority of them voice-to-voice calls, the spokesperson said. It imposed fines of 1.43 million euros. — *Dugie Standeford*

[Share Article](#)



Give your entire team critical **telecommunications intelligence** every business day.

Communications Daily offers an affordable multi-copy subscription plan that ensures all your key players are up to speed on business-critical regulatory activity, legislation, industry developments and competitive intelligence — **every business day.**

We have a distribution package that will meet your budget and business intelligence requirements. Contact your account representative today.

Why their own copy?

- Everyone gets detailed telecommunications news as it happens
- Significantly reduce your per-subscriber cost
- Eliminate hassles of forwarding/routing while maintaining copyright compliance

Call 800-771-9202

Let us help you find an affordable way to get *Communications Daily* on everyone's desk starting tomorrow.



Transaction
Network Services

TNS 2021 1H Robocall Investigation Report

Seventh Edition

By Transaction Network Services

September 2021



Executive Summary

3

Introduction

5

Primer on Robocalling

6

Methodology

7

Results and Analysis

8

How Carriers Should Address FCC Rule on Automatic Call Blocking

24

How Can Call Originators Get Customers to Answer the Phone?

26

Regulatory Updates—2021

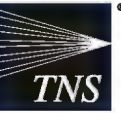
29

Industry Solutions to Combat Robocalling

32

Conclusions and Recommendations

35



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

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

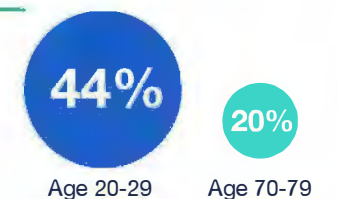
This seventh edition of TNS' Robocall Report continues the findings published beginning in 2018 and includes several new insights:

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

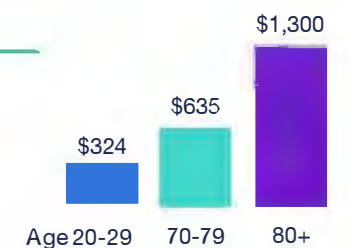
Industrywide:

- Consumers lost more than \$3.3 billion to fraud in 2020—an increase of nearly \$1.5 billion over 2019.¹
- Imposter scams topped the list of consumer complaints submitted in 2020 to the Federal Trade Commission's (FTC) nationwide Consumer Sentinel; debt scam reductions were second on the list followed by medical and prescription scams as the third highest complaint. These top three scams account for 27% of the complaints to the FTC.²
- The FTC saw a 36% increase in complaints received when comparing January-March of 2021 to the same period in 2020.³
- Younger people reported losing money to fraud more often than older people. In 2020, 44% of people in their 20s reported a loss to fraud, while only 20% of people in their 70s.⁴
- However, when people in their 70s did lose money, the amount tended to be higher: their median loss was \$1,300, compared to \$324 for people in their 20s.⁵

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 amounts to about \$3.3 billion annually



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

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



- The FCC saw a similar increase in complaints to the Do-Not-Call List, up 55% when comparing January-June of 2021 to the same period in 2020.⁶

FCC Complaints—Last 12 Months



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

Imposter Scams



About **1 in 5 People** Lost Money

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

Identity Theft Reports

2920% ↑

Government Benefits Applied For/Received

4% ↓

Evading the Law

Federal Trade Commission • ftc.gov/data

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



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

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

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

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

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

What valuable insights can your organization learn?

Introduction

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

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

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

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

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



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

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

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

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

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

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

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

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

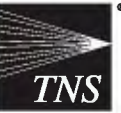
As of September 30, 2020, the registry had over 241 million active registrations, an increase of two million registrations from 2019.⁸

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

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



⁷<https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts>
⁸<https://www.ftc.gov/news-events/press-releases/2019/10/ftc-releases-fy-2019-national-do-not-call-registry-data-book>
⁹<https://ieeexplore.ieee.org/document/7546510/>



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

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

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

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

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

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

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

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

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

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

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

Layered Approach to Identifying Bad Actors

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



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.

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.

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



Positive Robocalls

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

Examples Include:

Public service announcement

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

Appointment confirmation

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

Prescription refills

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

Nuisance Robocalls

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

Examples Include:

Promotional offers

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

Solicitation

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

Accounts receivable

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

High-Risk Robocalls

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

Examples Include:

Social security scam

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

COVID-19 cures

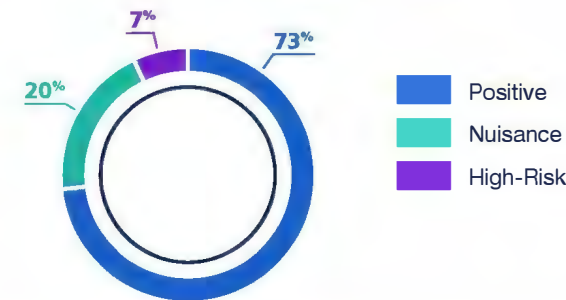
Calls selling fraudulent products that claim to prevent mitigate or detect the coronavirus.

Credit card interest scams

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

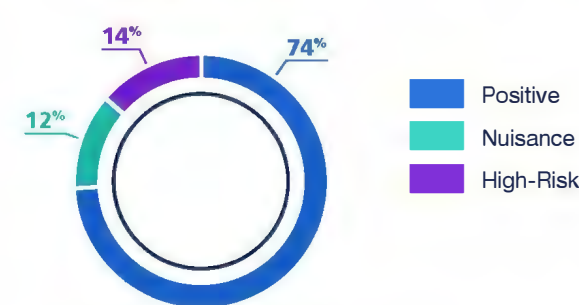
TNS found that 27% of the inter-carrier calls in 1H2021 were scored as unwanted, consistent with 2020. Unwanted represents non-positive calls or those that are scored as nuisance or high-risk.

Scoring by Category—1H2021



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

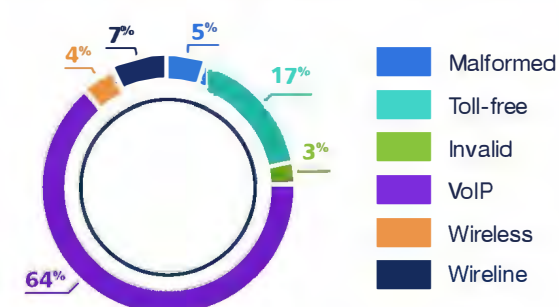
Scoring by Category—2020



Origination of Unwanted Calls

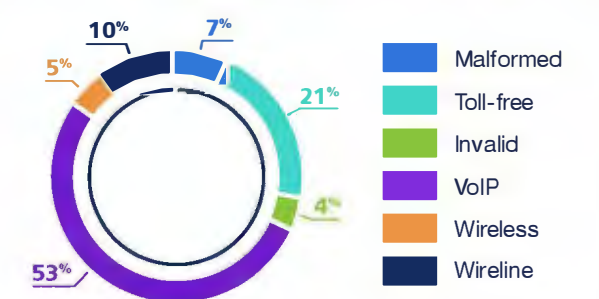
VoIP-originated calls accounted for 64% of the unwanted calls in 1H2021 by total volume, up significantly from 53% in 2020. Toll-free calls were the second highest at 17%.

Distribution of All Unwanted Calls—1H2021



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

Distribution of All Unwanted Calls—2020



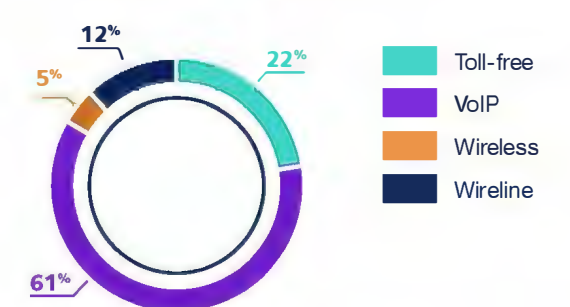
A provider that allows users to bring their own device and unbundles service so that direct inbound numbers may be purchased separately from outbound calling minutes are another source for bad actors.

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

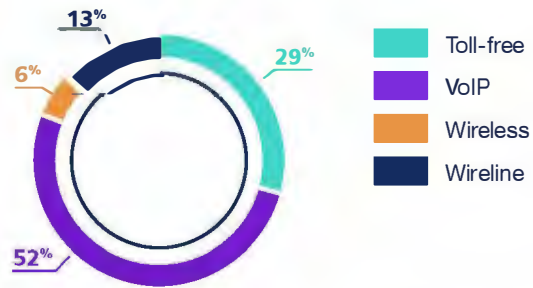
Providers that market "wholesale VoIP" allow any displayed number to be sent, as resellers will want their customer's numbers to appear.¹⁰

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

Distribution of Nuisance Calls—1H2021



Distribution of Nuisance Calls—2020

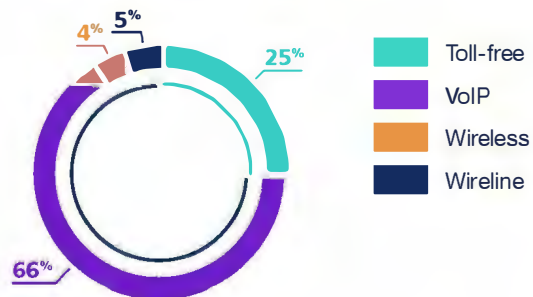


While there are legitimate reasons to modify the calling number, bad actors use this technique to hide their identity.

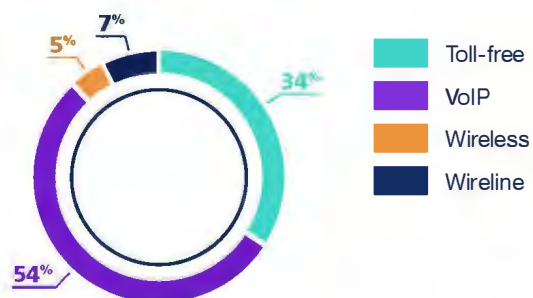
A malformed telephone number does not have 11 digits or does not start with 1. An invalid telephone number is well-formed but is not in a valid LERG block (NPA-NXX) and not in a valid toll-free area code.

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

Distribution of High-Risk Calls—1H2021



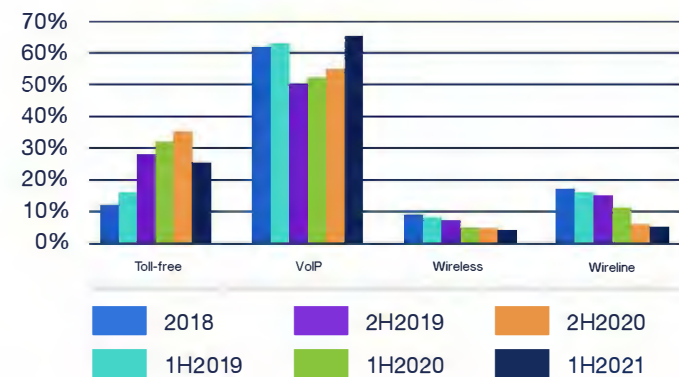
Distribution of High-Risk Calls—2020



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

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

Distribution of High-Risk Calls Over Time



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

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

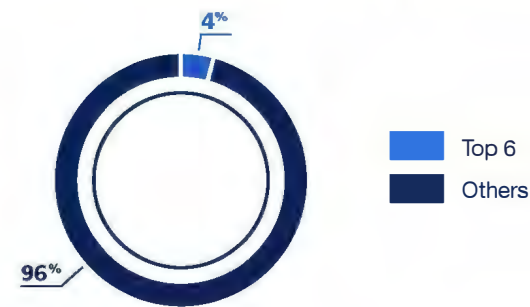
The FCC proposed to shorten by one year the extension for small voice service providers that originate an especially large number of calls. Those providers must implement STIR/SHAKEN in the IP portions of their networks no later than June 30, 2022. They believe this proposal will protect Americans from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

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

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

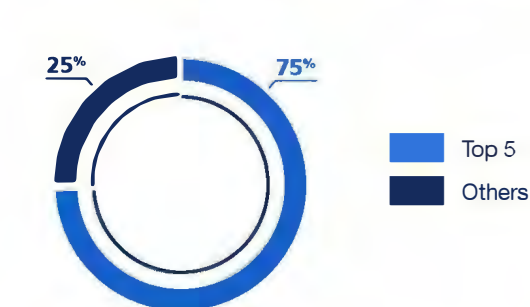
It is important to note that only 4% of the high-risk calls in 1H2021 originated from the top six carriers (AT&T, CenturyLink, Charter, Comcast, T-Mobile and Verizon). This is a significant drop from 11% in 2019 and down from 6% in 2020.

Telephone Numbers Placing High-Risk Calls



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

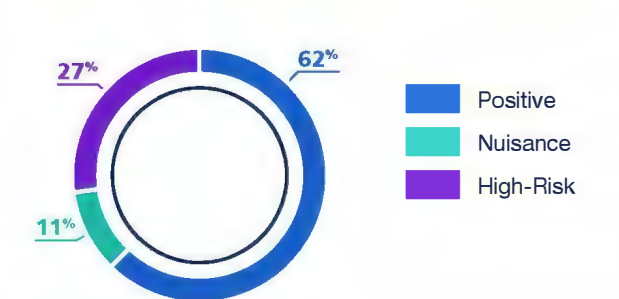
Telephone Number Resources—Total Calls



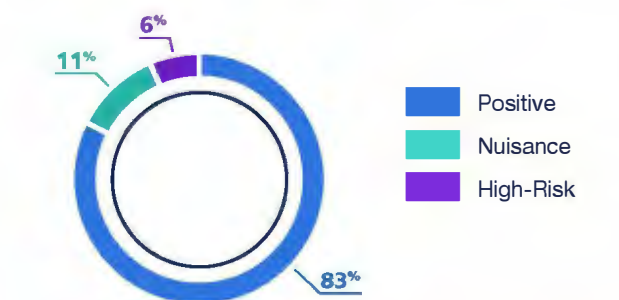
VoIP networks make it relatively easy to spoof caller ID. While most unwanted calls continue to originate from VoIP numbers, the percentage of *unwanted* VoIP calls went up to 38% in 1H2021, more than double from 2020 (17%).

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

Scoring of VoIP Telephone Numbers—1H2021



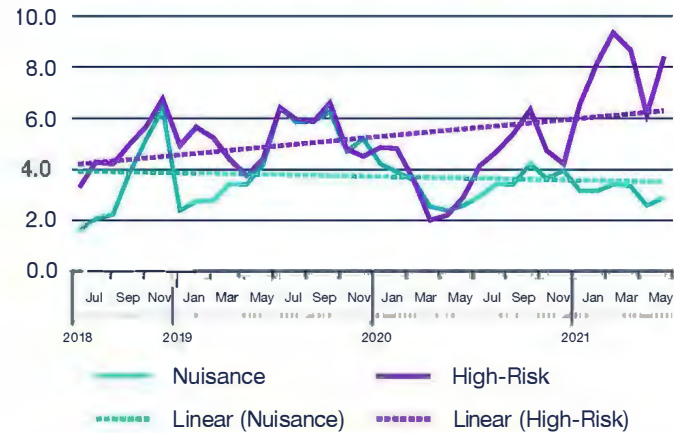
Scoring of VoIP Telephone Numbers—2020



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

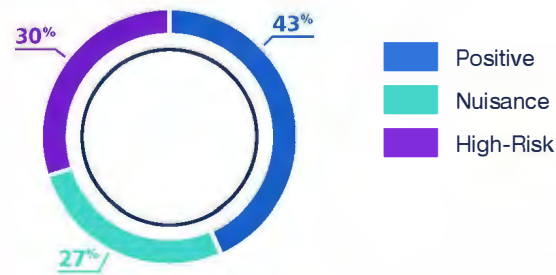
Bad actors are using VoIP originating networks. The number of nuisance calls, on a per subscriber basis, coming from a VoIP number, has stayed relatively flat to slightly declining. However, the number of high-risk calls, per subscriber, has more than doubled, up 123% in comparing 1H2021 to 1H2020.

Unwanted Calls per Telephone Number—VoIP

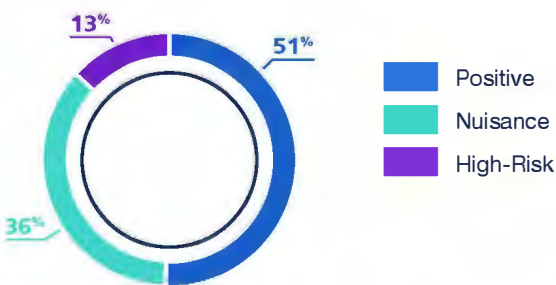


The percentage of unwanted calls coming from toll-free numbers has increased from 49% in 2020 to 57% in 1H2021.

Scoring Distribution Toll-Free Calls—1H2021



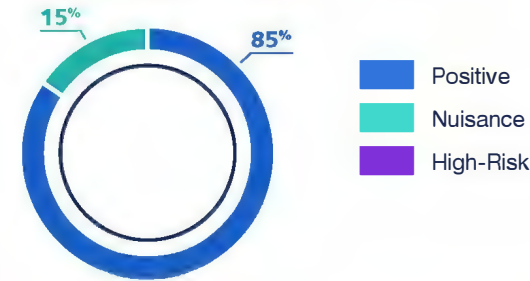
Scoring Distribution Toll-Free Calls—2020



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

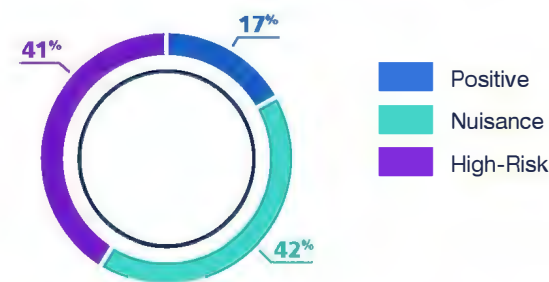
Of the top 10 toll-free numbers in 1H2021 in terms of call volume, 83% of the calls are scored as positive from TNS, up from 71% in 1H2020. This jump is due to an increase in enterprise and government agencies registering toll-free numbers.

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



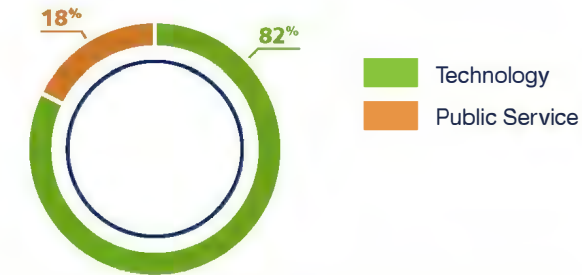
The crowd-sourced data from the top 10 toll-free numbers, however, is overwhelmingly considered nuisance or high-risk by the subscriber.

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



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

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



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

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

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

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

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

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

Termination of Unwanted Calls

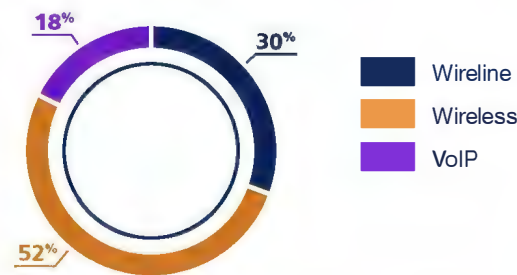
Total calls to wireless telephone numbers have now exceeded calls to wireline and VoIP telephone numbers. This phenomenon isn't surprising with cord-cutting of home telephone service continuing and more reliance on smartphone devices by younger consumers.

Calls to wireless telephone numbers now exceed wireline and VoIP combined



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

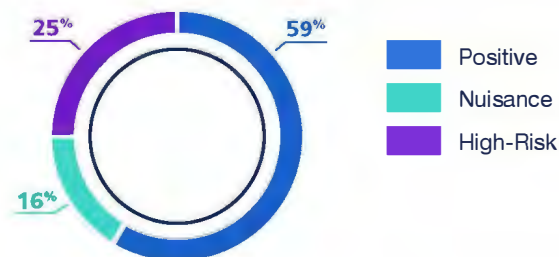
Total Call Distribution Called Telephone Number—1H2021



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

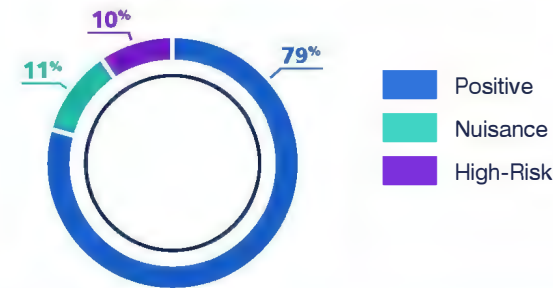
While much of the attention goes towards robocalls to mobile phones, TNS finds that 41% of wireline calls in 1H2021 were unwanted, compared to 21% to wireless numbers.

Distribution of Scoring for Wireline Telephone Numbers—1H2021



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

Distribution of Scoring for Wireless Telephone Numbers—1H2021

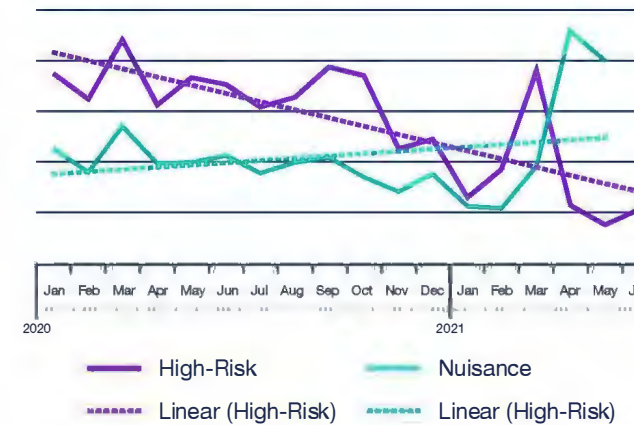


Wireline twice as likely to receive an unwanted call than wireless

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

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

Wireline Unwanted Call Trend



Wireless Unwanted Call Trend



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

Opt-in subscriber services may be impacting bad actors

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

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

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

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

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

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



¹⁴<https://docs.fcc.gov/public/attachments/DA-20-772A1.pdf>

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

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

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

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

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

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

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

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

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

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

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

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

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

Top Scams

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

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

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

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

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

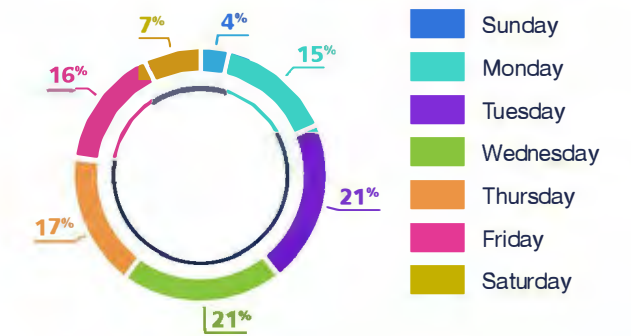
Home buying scam—The scams begin by asking what kind of property you own and if you are interested in selling it, attempting to make the call sound legitimate. Then they will make a bogus offer, possibly one you cannot refuse. The catch—there is an “administrative fee” which, after being paid, results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

Political scam—These scams take on three forms:

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

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

Day of Week for Unwanted Calls—1H2021



Donation scam had highest volume on heaviest day in 1H2021

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

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

The Federal Trade Commission (FTC) has received 2,095 fraud incident reports for charitable contributions totaling \$2.8 million in the first quarter of 2021.¹⁶



FTC Consumer Sentinel Network

Charitable Solicitations Year: 2021 YTD

Fraud Facts at a Glance

of Fraud Reports: **2,095**

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

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

Median Loss Reported: **\$450**

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

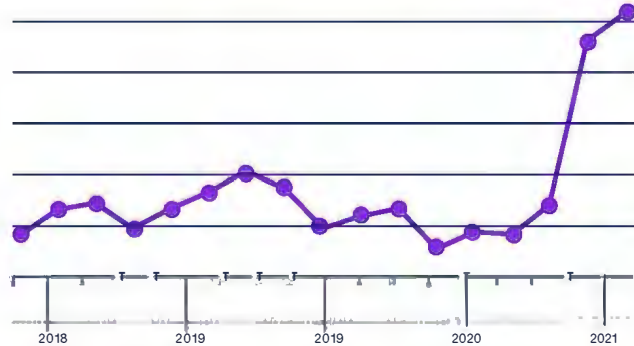
Top Contact Method: **Social Media**

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

Federal Trade Commission • ftc.gov/data

The total number of reports and dollar loss submitted to the FTC has grown dramatically in 2021.¹⁷

Fraud Reports by # of Reports Charitable Solicitations



The FTC provides important questions to ask a caller regarding the charity including:¹⁸

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

In addition, the callers must follow certain rules:¹⁹

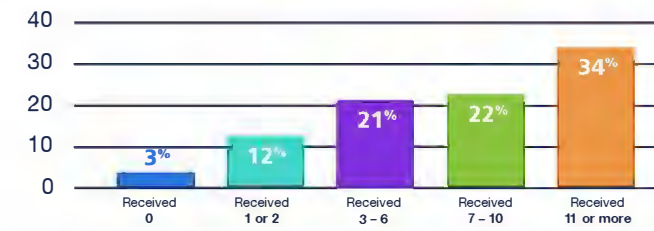
- They can't call you before 8 am or after 9 pm
- They must tell you the name of the charity and tell you if the reason they're calling is to seek a donation
- They can't deceive you or lie about:
 - The fundraiser's connection to the charity
 - The mission or purpose of the charity
 - Whether a donation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

A TNS survey in 1H2020 found that 53% of US *senior citizens* believe robocallers tried to scam them out of personal information in 2019; and nearly as many (47%) reported that they were targets of financial scams in 2018.²⁰

Additional findings from the survey are the following:

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

Robocalls per Week



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

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

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

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

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

Scammers Become More Sophisticated; Change Robocall Methods and Tactics

Scammers Shift to VoIP Networks

- With Tier-1 high-risk call volume down, robocallers are turning to VoIP networks, which account for the largest share of unwanted calls.
- 66% of all high-risk calls and 61% of all nuisance calls originate from VoIP telephone numbers - two of highest sources of spam.
- The percentage of unwanted calls on VoIP networks increased to 38% in the first half of 2021, rising from 23% in the first half of 2020.

Robocallers Double Down on Home Wireline Phones

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

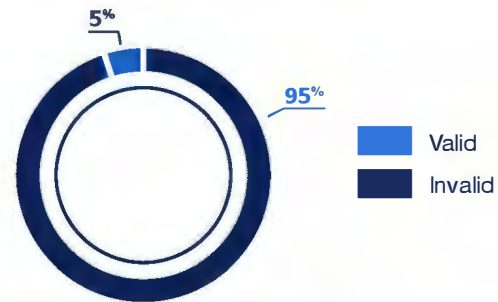
Because wireline numbers are now twice as likely to receive unwanted calls as wireless numbers is a reminder that robocalls aren't just a mobile phone problem.



Invalid/Unallocated Number Use

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

Unwanted Calls by Valid/Invalid NPA-NXX



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

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

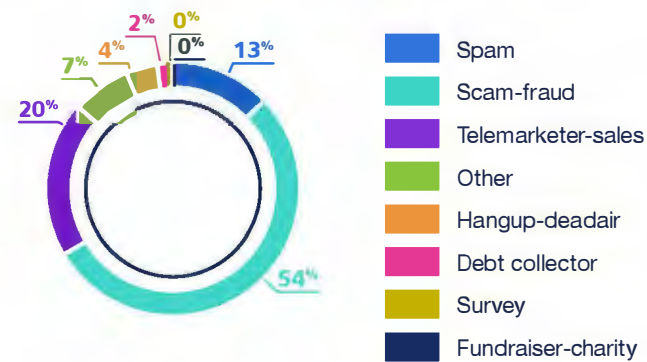
Crowd-Sourced Statistics

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

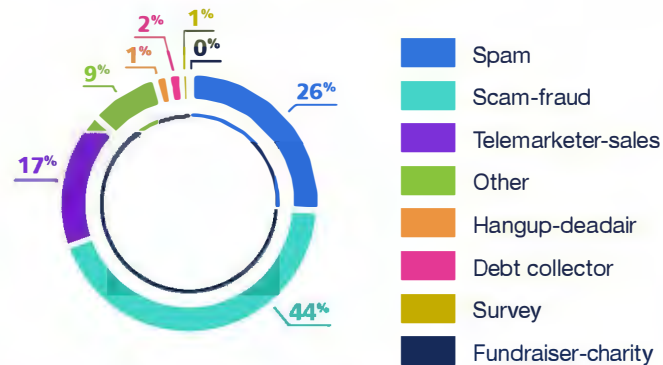
Enhanced Caller ID identifies callers or texters with their names displayed directly in the incoming call screen and message threads, even if their number is not in contacts.

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

Crowd-Sourced Feedback by Major Category—1H2021



Crowd-Sourced Feedback by Major Category—2020



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

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



Neighbor Spoofing

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

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

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

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

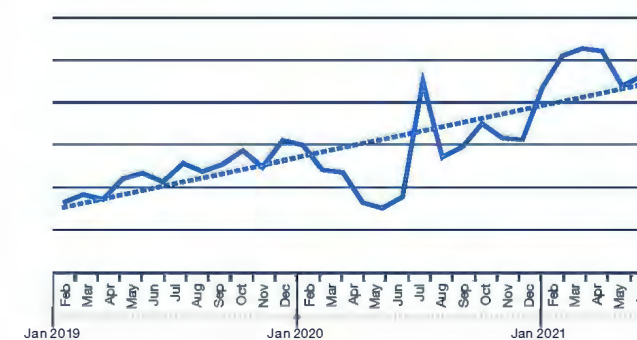
TNS has observed an increase in bad actors that are using low-volume spamming across a large amount of telephone numbers while attempting to avoid analytics engines. The two most common techniques involve either mimicking call patterns of a small to medium sized business and spreading calls over many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

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

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

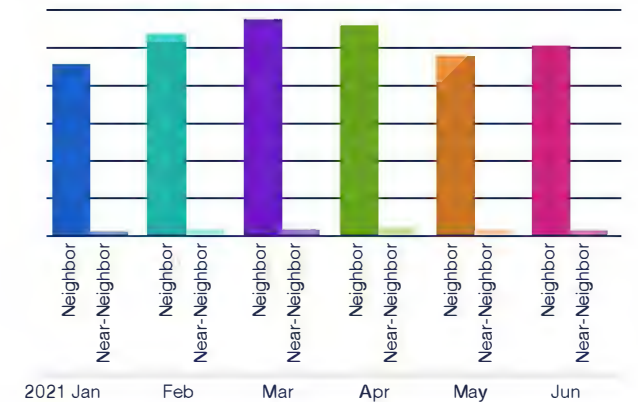
However, bad actors are using neighbor spoofing less due to implementation of STIR/SHAKEN on the major wireless networks. Instead, they have shifted to near-neighbor spoofing where the area codes are the same, but not the first five or six digits. TNS has seen a remarkable increase of 127% in near-neighbor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

Near-Neighbor Spoofing Events per Subscriber



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

Neighbor Spoofing vs. Near-Neighbor Spoofing



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

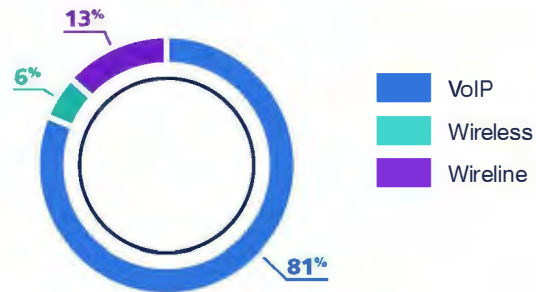
Snowshoe spamming is difficult to detect for over-the-top (OTT) applications. To be effective an application must be integrated with the network and see the cross-carrier events of both the calling number and the called number.

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

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

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

Near-Neighbor Spoofing by Line Type—1H2021

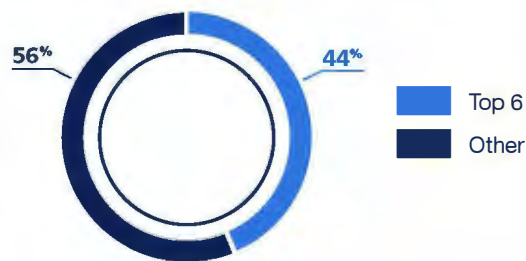


STIR/SHAKEN Attested Traffic

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

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

Cross-Carrier Traffic Among Tier 1 Carriers



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

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

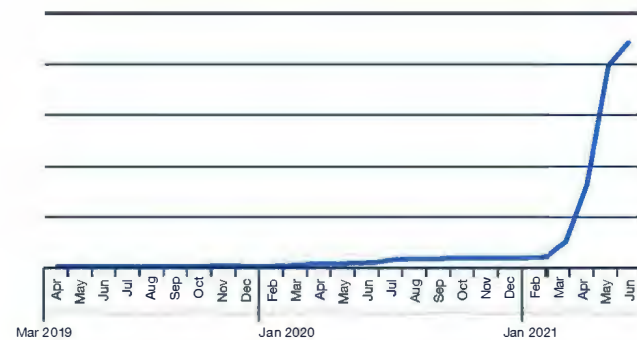
Full Attestation (A)—The service provider has authenticated the calling party and they are authorized to use the calling number.

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

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

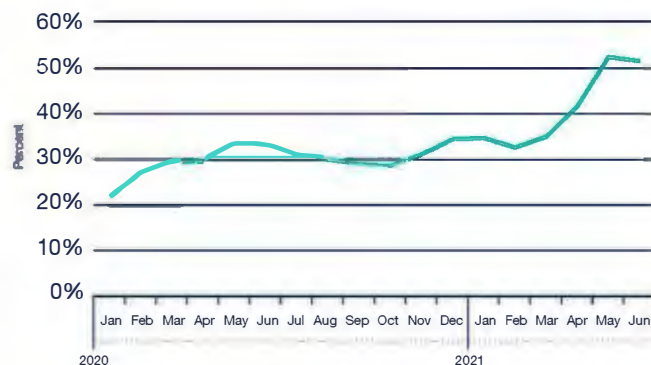
The amount of inter-carrier traffic that TNS has seen shows attestation has continued to grow dramatically in 1H2021.

Inter-Carrier Signed STIR/SHAKEN Traffic



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

STIR/SHAKEN Traffic to Total Traffic



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

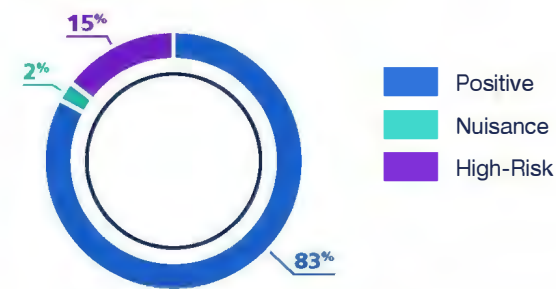
Canadian Results

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

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

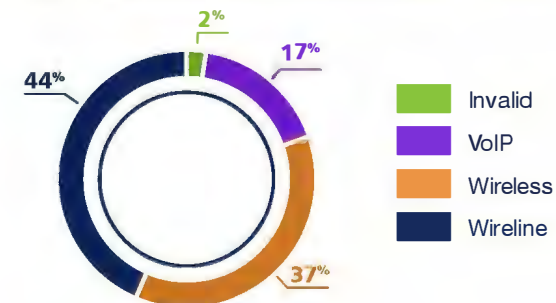
TNS found less than 20% of Canadian inter-carrier calls in 1H2021 were scored as unwanted, consistent with 2020 and 2019.

Scoring by Category—Canadian Telephone Numbers—1H2021



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

Distribution of Unwanted Calls from Canadian Telephone Numbers—1H2021



International Results

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

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

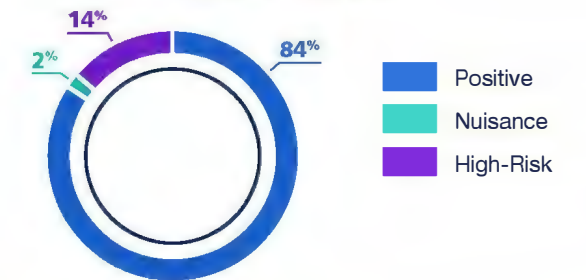
Many of the high-risk calls that come from international numbers are associated with **Wangiri** attacks.

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

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

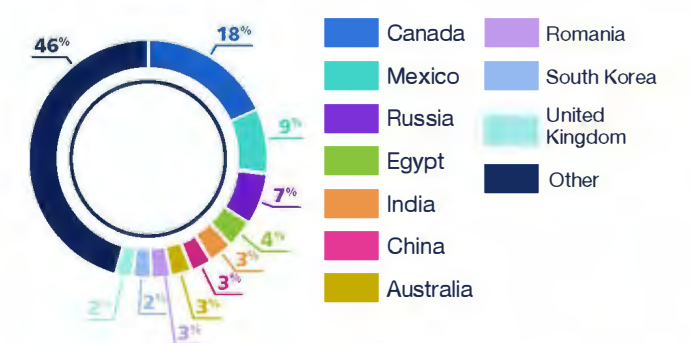
Every time you call, you will be charged high international rates or other connection fees. The bad actor profits from those fees.

Scoring by Category—International Telephone Numbers



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

Unwanted Calls from Numbers Outside US



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



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

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

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

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

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

Recognize Robocalls are Not Created Equal

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

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

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

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

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

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

It's All About Data Analytics

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

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

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

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

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

Prioritize Consumer Education

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

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

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

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

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

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

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

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

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

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

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

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

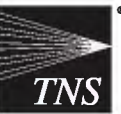
Automatic call blocking is part of a broader and necessary effort to more aggressively combat robocalls and shift much of the burden and associated frustration away from subscribers.

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

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



²¹ <https://www.tns.com/en-us/insights/consumer-sentiment/entry/option-to-combat-robocalls>
²² <https://www.tns.com/en-us/insights/call-survey-online/entry/option-to-combat-robocalls>





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

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

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

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

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

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

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

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

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

Don't Use One Main Calling Number for Multiple Uses

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

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

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

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

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

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

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

Provide a Consistent Calling Name Profile that Matches Context

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

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

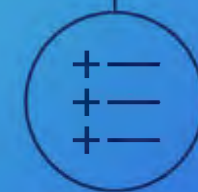
Document Normal Calling Patterns

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

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

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

Enterprises should work with analytics providers to register their calling campaigns



Don't Call Unassigned Numbers Frequently

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

Comply with DNC Lists, TCPA and FDCPA

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

Branded Calling

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

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

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

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

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

Branded Calling Study

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

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



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

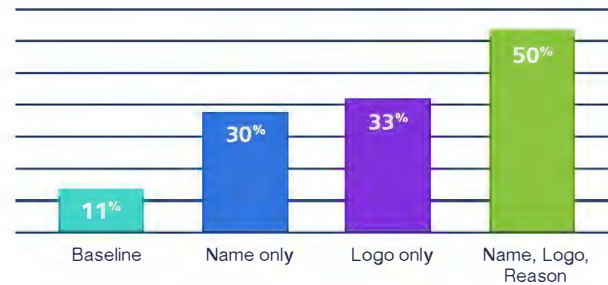
Consumers are most interested in receiving calls from healthcare services, financial institutions and delivery services.

Consumers Most Interested in Calls From



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

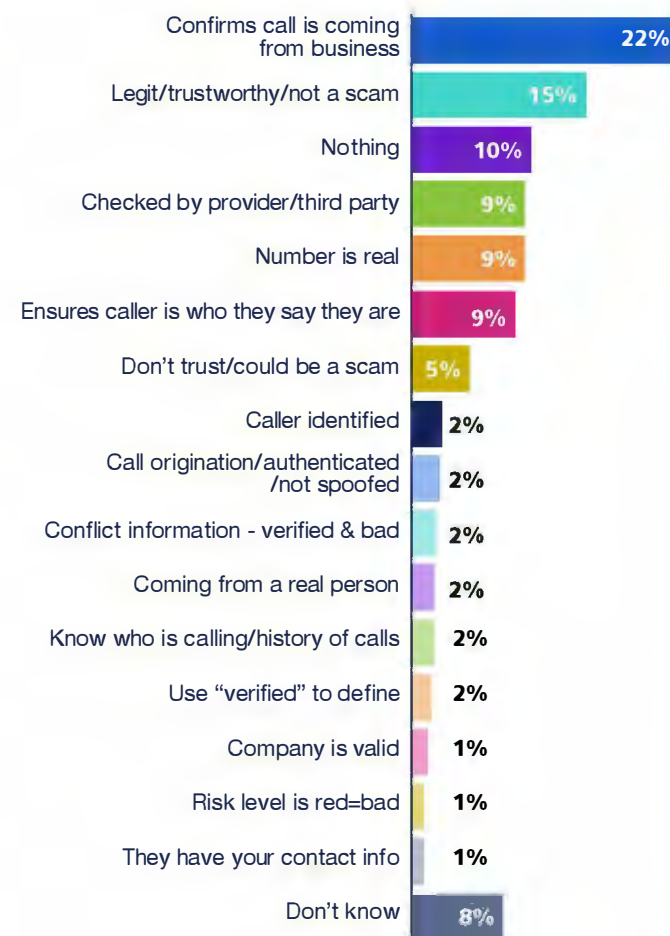
Percent Likely to Answer



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.

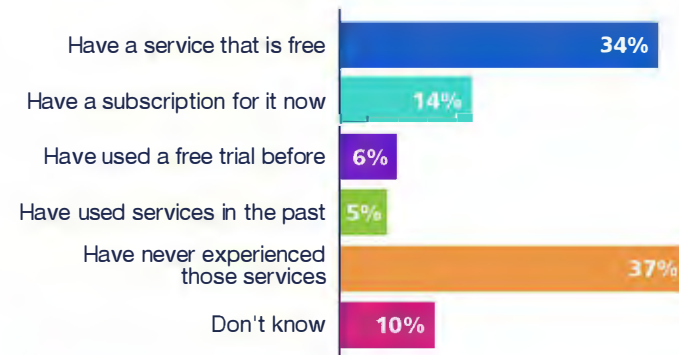
Interpretations of “Caller Verified” Verstat



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

You can refer to the *2021 Robocall Investigation Report, Sixth Edition* for the actions taken in the second half of 2020.

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

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

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

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

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

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

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

Robocall Mitigation Database Opens, Filing Instructions and Deadlines

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

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

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

FCC Announced a New Webpage to Collect TRACED Act Actions

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



Hardware and Software

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

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

Blacklists and Whitelists

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

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

Landline Call Blockers

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

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

Some models also can create a user-generated whitelist³⁸.

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

Crowdsourcing

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

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

In 2013, hackers gained access to one OTT provider database of known genuine numbers, highlighting the danger of centralizing this information.^{39, 40}

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.⁴¹

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

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

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

STIR/SHAKEN

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

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

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

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

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

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

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

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

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

Real-Time Analytics

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

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

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

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

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

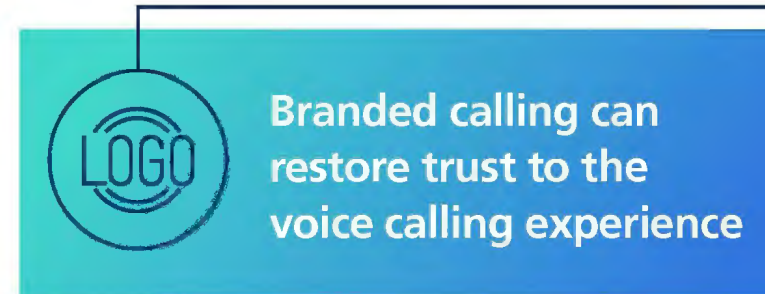
Machine learning is a method used to devise complex models and algorithms that lend themselves to predictive analytics. The analytical models allow data scientists to produce reliable and repeatable decisions while also uncovering hidden insights through learning from historical relationships and trends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

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

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

Enterprise Response to Analytics

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

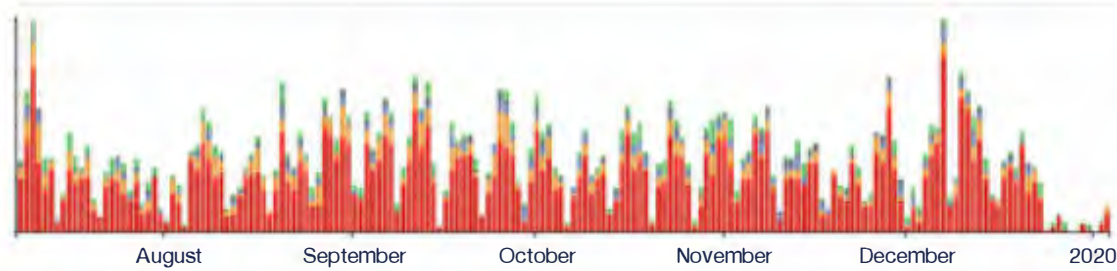


The industry is implementing tools such as **Branded Calling**, where a logo and other business information may be displayed for legitimate calls.

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

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

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

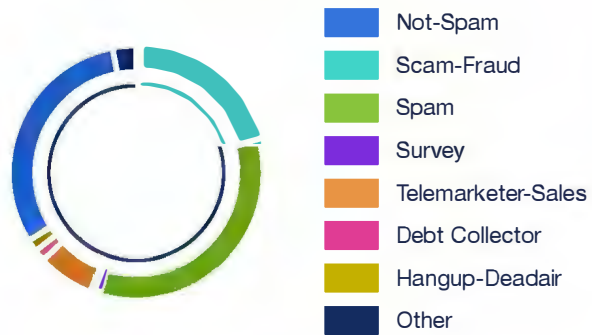


Above is an example showing mixed customer feedback.

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

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

Category Distribution



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

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

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

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

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

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

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

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

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

A layered approach is most effective in combating robocalls





**Transaction
Network Services**

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

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

©2021 Transaction Network Services. All rights reserved. The information contained within this document is the confidential information of Transaction Network Services. Disclosure, distribution or use of this document is not permitted outside of Transaction Network Services without written permission. Subject to non-disclosure obligations of Transaction Network Services employees and contractors.

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



2022 Robocall Investigation Report

Eighth Edition

By Transaction Network Services

March 2022

Table of Contents

Executive Summary

3

Introduction

5

Primer on Robocalling

6

Methodology

7

Results and Analysis

8

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

23

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

25

Regulatory Updates—2H2021

28

**Industry Solutions to
Combat Robocalling**

32

**Conclusions and
Recommendations**

35



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

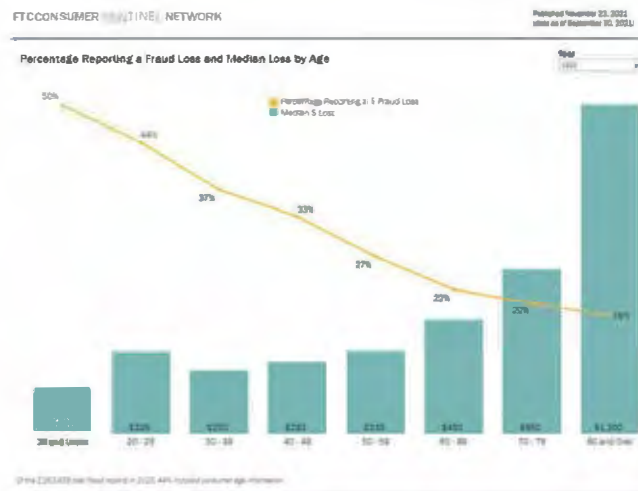
TNS' Call Guardian®, the industry-leading big-data analytics engine, has gained insights and reputation data on almost two billion active phone numbers by analyzing over 1.5 billion daily call events across hundreds of carriers.

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

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

Industrywide,

- Consumers lost more than \$3.5 billion to fraud in the first three-quarters of 2021 – an increase of nearly \$1.7 billion over 2019.¹
- Imposter scams topped the list of consumer complaints submitted in 2021 in terms of number reported and total dollar loss to the Federal Trade Commission's (FTC) nationwide Consumer Sentinel; investment related fraud was second on the list in total dollar loss followed by online shopping as the third highest total. These top three scams account for 82% of the total dollar loss according to the FTC.²
- The FTC saw a 24% increase in complaints to the Do-Not-Call Registry received when comparing January-September of 2021 to the same period in 2020.³
- Younger people reported losing money to fraud more often than older people. In first nine months of 2021, 50% of people 19 and under reported a loss to fraud, while only 18% of people in their 70s.⁴
- However, when people in their 80s did lose money, the amount tended to be higher: their median loss was \$1,300, compared to \$326 for people in their 20s.⁵



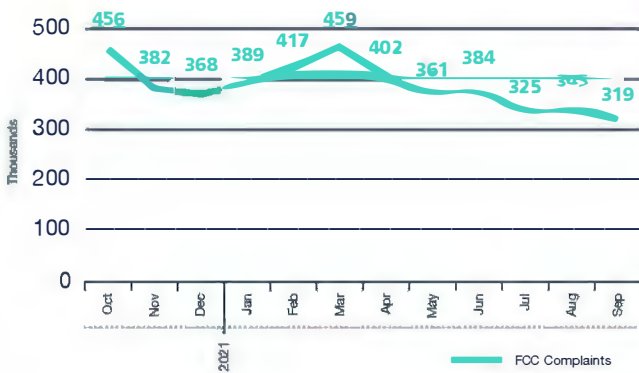
<https://www.ftc.gov/app/privacy/federal-trade-commission-will-use-big-view-ai-sentinel-reports-top-reports>
<https://www.ftc.gov/app/privacy/federal-trade-commission-will-use-big-view-ai-sentinel-reports-top-reports>
<https://www.ftc.gov/app/privacy/federal-trade-commission-will-use-big-view-ai-sentinel-reports-top-reports>
<https://www.ftc.gov/app/privacy/federal-trade-commission-will-use-big-view-ai-sentinel-reports-top-reports>
<https://www.ftc.gov/app/privacy/federal-trade-commission-will-use-big-view-ai-sentinel-reports-top-reports>

Fraud amounted to \$3.5 billion through September 2021



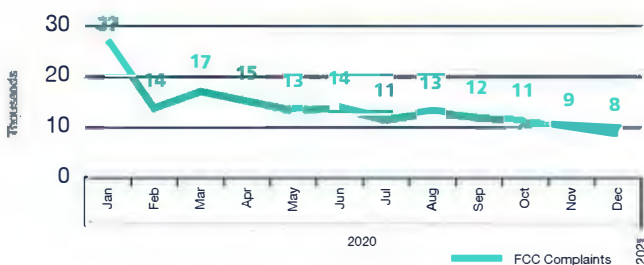
Fraud has become easier for criminals as technology, like VoIP calling, has enabled both spoofing numbers and low cost robo-dialing. A late 2021 TNS study found 43% of consumers still answer calls from unknown numbers for fear of missing an important call, which is why nearly six in 10 (59%) of those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

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



- However, the FCC saw a decrease in in complaints to the Don-Not-Call List of 8% when comparing 2021 to 2020.⁹

FCC Complaints—Last 12 Months



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

Imposter Scams



About **1 in 5 People** Lost Money

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

Identity Theft Reports

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

4% **Evading the Law**

Federal Trade Commission • ftc.gov/data

TNS estimates that nearly 80 billion unwanted calls were placed in the last 12 months. *Unwanted* represents non-positive calls or those that are scored as nuisance or high-risk.



Nearly 80 billion unwanted calls in last 12 months

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

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

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

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

⁹<https://endat.ftc.gov/ons/nc/ConsumComplaintData/UnwantedCalls/vakf-Be-ist>

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

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

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

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

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



Primer on Robocalling

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

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

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

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

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

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

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

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

As of September 30, 2020, the registry had over 241 million active registrations, an increase of two million from 2019.⁸

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

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

⁷<http://www.ftc.gov/consumers/guides/stop-unwanted-robocalls-and-text>
⁸<https://www.ftc.gov/news-press/releases/2018-10-ftc-releases-fy-2018-national-donot-call-registry-data-block>
⁹<https://www.ftc.gov/document/7516630/>



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

Call Guardian analyzes over 1.5 billion daily call events across hundreds of carriers and creates robocall scoring and categorization on this vast data pool.

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

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

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

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

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

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

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

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

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

TNS Network Data Sources

Results of Over Billions of Signaling



Database Transactions per Day from Over 500 Operators

Layered Approach to Identifying Bad Actors



DNC List, FCC Complaint Data



DNO, Invalid, Unassigned, Unallocated Telephone Numbers



INP Data, NPAC Data, LERG Data, Toll-Free Routing Data



VoLTE / VoIP Peering



Crowd-Source Data, Honeypot Data



Enterprise Data



STIR/SHAKEN Parameters



Fraud, Spam and Premium Rate Called Numbers



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



Results and Analysis

Reputation Category and Scoring

TNS uses reputation categories to score common call behavior. This reputation scoring is comprised of categories that are indicative of legitimate, abusive, fraudulent and unlawful call behavior – inclusive of any call placed via auto-dialer or manually dialed.

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

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



Positive Robocalls

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

Examples Include:

Public service announcement

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

Appointment confirmation

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

Prescription refills

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

Nuisance Robocalls

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

Examples Include:

Promotional offers

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

Solicitation

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

Accounts receivable

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

High-Risk Robocalls

High-risk calls typically cause emotional distress while the severity of harm often includes loss of money, invasion of privacy and identity theft, all hallmarks of a major crime. These callers are preying on consumers and have one of the following characteristics:

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

Examples Include:

Social security scam

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

COVID-19 cures

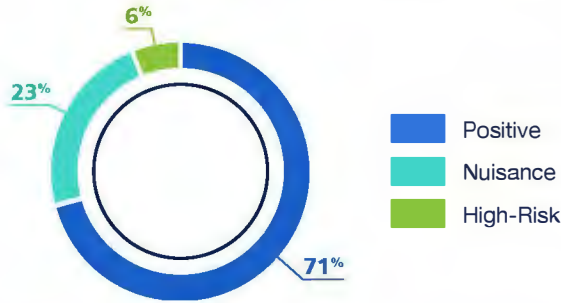
Calls selling fraudulent products that claim to prevent mitigate or detect the coronavirus.

Credit card interest scams

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

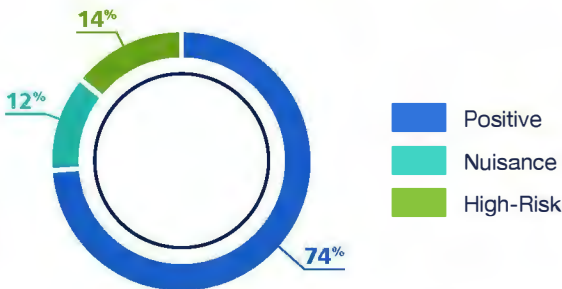
TNS found that 29% of the inter-carrier calls in 2021 were scored as *unwanted*, consistent with 2020, but slightly higher which says the problem isn't going away.

Scoring by Category—2021



The past year has shown a noticeable shift in the mix of unwanted calls with nuisance calls making up a much larger portion. Nuisance calls were 12% in 2020 compared to 23% for all of 2021 and only 20% in first half of 2021.

Scoring by Category—2020

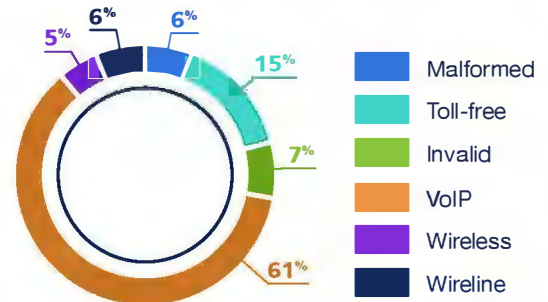


Origination of Unwanted Calls

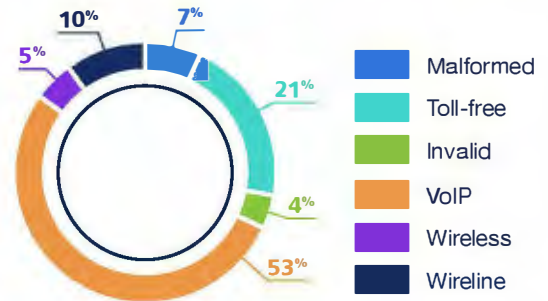
VoIP calls represent telephone numbers utilized by the cable operators (MSOs) and VoIP providers.

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

Distribution of All Unwanted Calls—2021



Distribution of All Unwanted Calls—2020



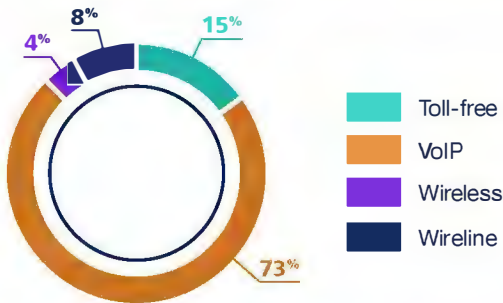
Providers that allow users to bring their own device and unbundle service so that direct inbound numbers may be purchased separately from outbound calling minutes are another source for bad actors.

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

Providers that market "wholesale VoIP" allow any displayed number to be sent, as resellers will want their customer's numbers to appear.¹⁰

Nuisance calls continue to be led by VoIP telephone numbers and the share of nuisance calls coming from VoIP telephone numbers increased from 52% of the calls in 2020 to 73% of the calls in the first half of 2021.

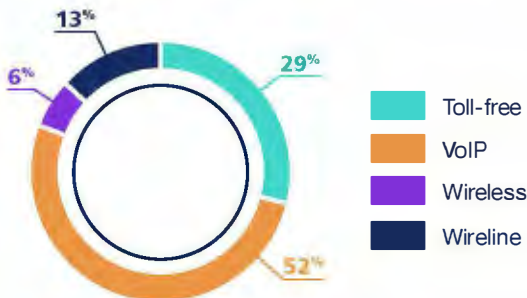
Distribution of Nuisance Calls—1H2021



VoIP calls are nearly three-quarters of the nuisance calls



Distribution of Nuisance Calls—2020

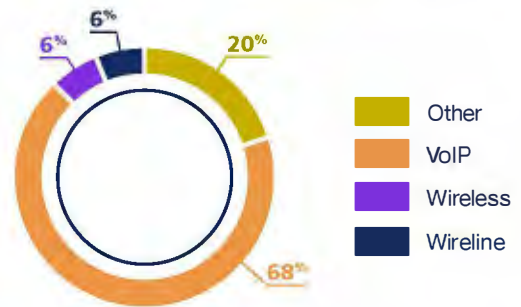


VoIP numbers, in 2021 remain the largest source (68%) of high-risk calls, up significantly from 54% in 2020. Invalid and malformed numbers are in the "other" category along with toll-free numbers and are the second highest source of high-risk calls in the charts below.

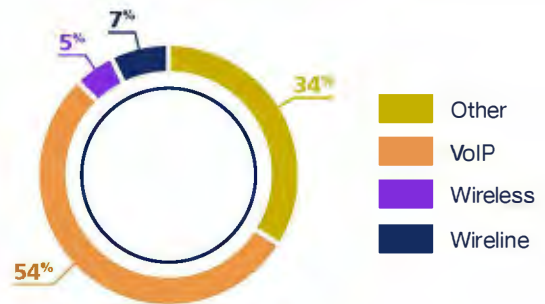
While there are legitimate reasons to modify the calling number, bad actors use this technique to hide their identity.

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

Distribution of High-Risk Calls—2021



Distribution of High-Risk Calls—2020

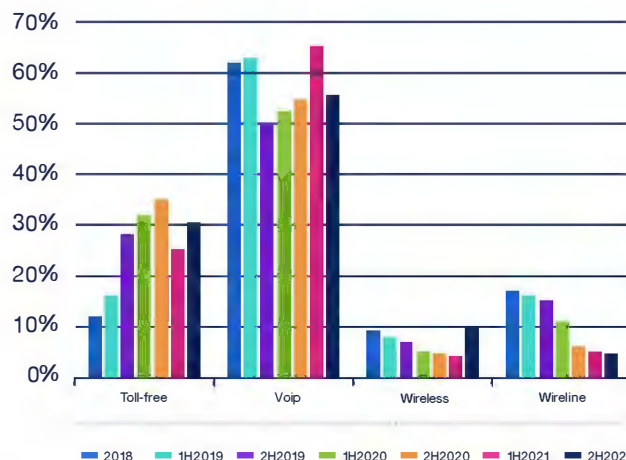


Spoofing of wireless telephone numbers had been declining from 2020 to 1H2021, however it increased in the second half of 2021. Bad actors have shifted to near-neighbor spoofing where the area codes are the same, but not the first five or six digits which is being done primarily by VoIP numbers.

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

Donations are a great way to support causes you hold close to your heart, but scammers are notoriously good at tricking those who are passionate about an issue and want to help through funding, so it is important to be very cautious when making donations. Some legitimate non-profit organizations have confirmed they do not solicit donations over the phone. For example, the National Police Foundation does not solicit donations from anyone via phone, according to their [website](#). There is no safe way to confirm the identity of the caller, so never give your credit card, address or other personal information over the phone.

Distribution of High-Risk Calls Over Time



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

The FCC proposed and approved to shorten by one year the extension for small voice service providers that originate an especially large number of calls. Those providers must implement STIR/SHAKEN in the IP portions of their networks no later than June 30, 2022, for non-facilities-based providers. The FCC will further require any small voice service providers that the Enforcement Bureau suspects of originating illegal robocalls and that fails to mitigate such traffic upon Bureau notice or otherwise fails to meet its burden under section 64.1200(n)(2) of its rules, to implement STIR/SHAKEN within 90 days of that determination unless sooner implementation is otherwise required.^{11, 12}

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

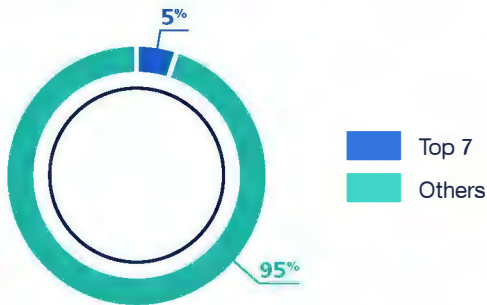
In a recent filing to the FCC, USTelecom indicated that most Industry Traceback Group (ITG) tracebacks identify smaller, VoIP-based providers as the originator for illegal robocalls whether those calls originate in the US or abroad. Tracebacks seldom conclude that a large provider originated the robocall,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

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

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



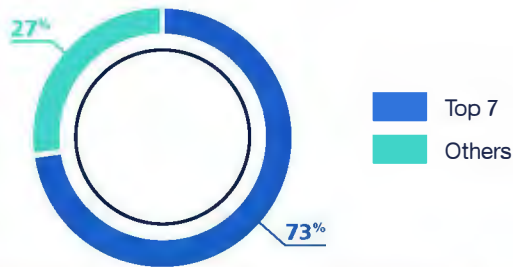
Telephone Numbers Placing High-Risk Calls—2021



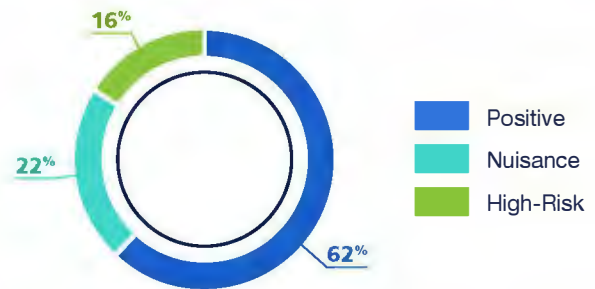
The Tier-1s account for 73% of the total number of calls in 2021, up slightly from 67% in 2020. However, the Tier-1s are a declining percentage of high-risk calls.



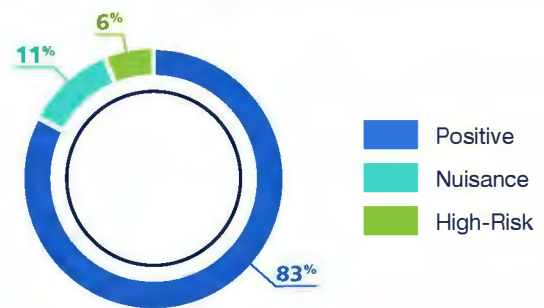
Telephone Number Resource Total Calls—2021



Scoring of VoIP Telephone Numbers—2021



Scoring of VoIP Telephone Numbers—2020



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



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

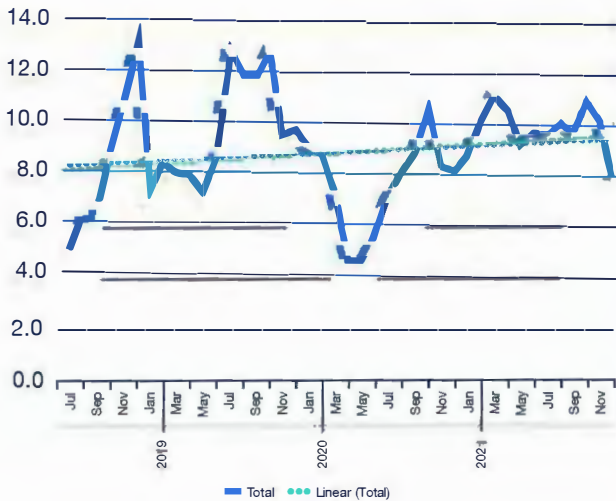
TNS believes this is due to low-volume spammers using VoIP to generate robocalls that are being purchased by wholesale VoIP providers.



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

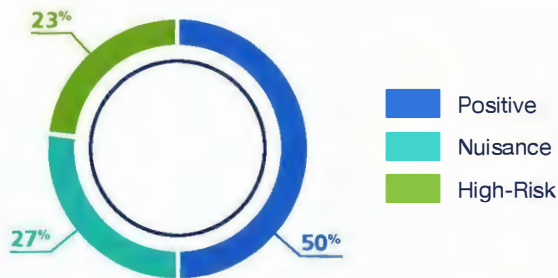
Bad actors are using VoIP networks to originate calls. The number of nuisance calls, on a per subscriber basis, coming from a VoIP number, has stayed relatively flat to slightly declining. However, the number of high-risk calls, per subscriber, has more than doubled, up 123% in comparing 1H2021 to 1H2020.

Unwanted Calls per Telephone Number—VoIP

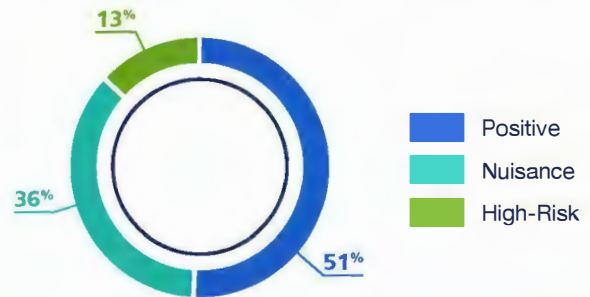


The percentage of unwanted calls coming from toll-free numbers was similar with 49% unwanted in 2020 to 50% in 2021.

Scoring Distribution of Toll-Free Calls—2021



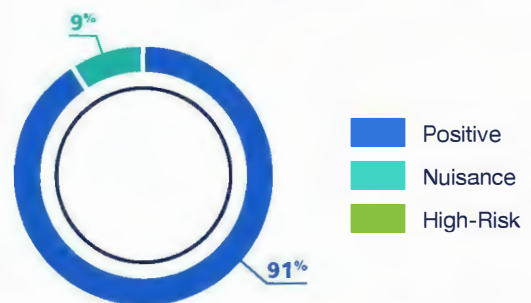
Scoring Distribution of Toll-Free Calls—2020



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

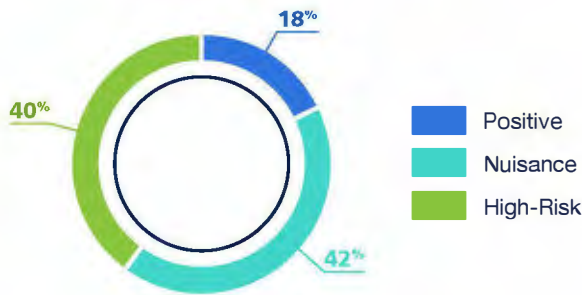
Of the top 10 toll-free numbers in 2021 in terms of call volume, 91% of the calls are scored as positive from TNS, up from 71% in 1H2020. This jump is due to an increase in enterprise and government agencies registering toll-free numbers.

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



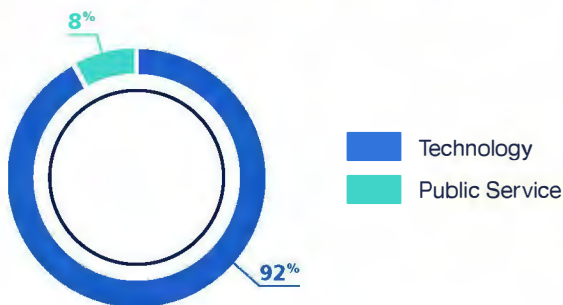
The crowd-sourced data from the top 10 toll-free numbers, however, is overwhelmingly considered nuisance or high-risk by the subscriber.

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



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

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



The perceived risk of missing an important phone call was heightened during the COVID-19 pandemic in 2020 and 2021. For example, one of the biggest challenges contact tracers faced – especially in the early months of the pandemic – was an unexpected one: robocalls. Scammers spoofing legitimate government and health agency phone numbers tricked people into surrendering money or personal information. The fact is the public has been conditioned over the past several years to stop answering calls from unknown numbers, leading them to mistrust or not answer legitimate contact tracing efforts. Because of this, wireless carriers, government health agencies and industry leaders prioritized efforts to authenticate call identification information for consumers and improve answer call rates for legitimate contact tracing calls.


The challenge faced by contact tracing efforts is simply the latest – albeit higher stakes – manifestation of the extent to which consumers have been hammered with a variety of increasingly convincing robocalls in the past few years, including many claiming to be well-known companies like Apple and Amazon. Most, if not all, of Apple’s store phone numbers have been spoofed at some point. The calls sound legitimate, provide a secondary “customer service” number to call and immediately begin harassing the victim.

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

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

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



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

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

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

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

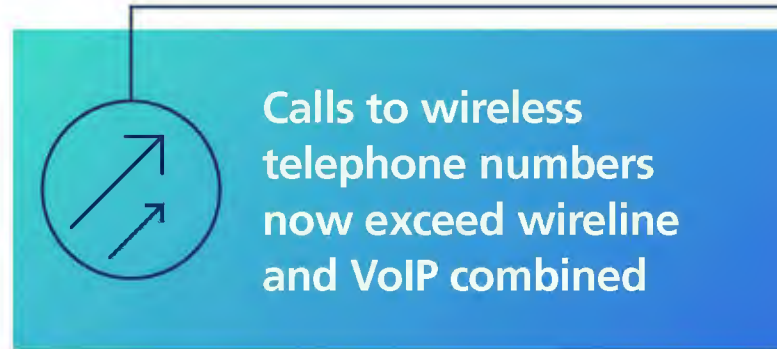
A RESPOG is the entity that assigns a toll-free number to a customer and is the only entity that can authenticate that a customer has the right to use a toll-free number. Unless a Resp Org is also a service provider, it is not involved in originating a call and previously was not able to provide the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

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



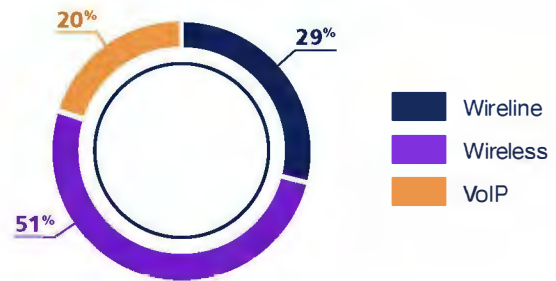
Termination of Unwanted Calls

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



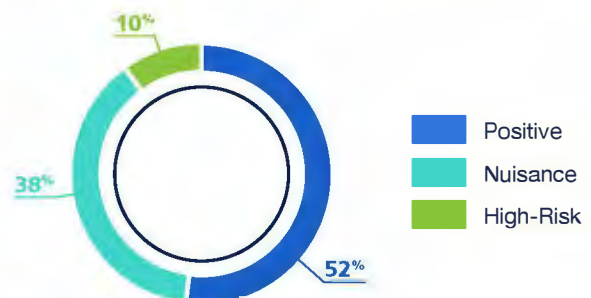
Calls to wireless telephone numbers account for 51% of the total call volume for 2021, up from 46% in 2020. Call volume to wireline has decreased 6% while call volume to wireless has increased 16% comparing 2021 to 2020.

Total Call Distribution Called Telephone Numbers—2021



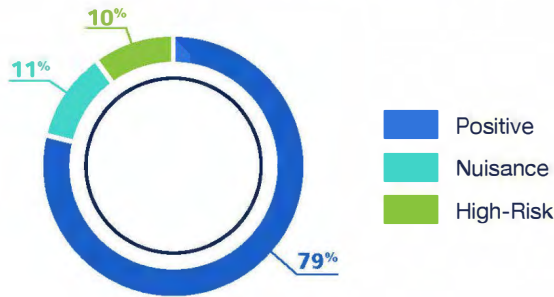
While much of the attention goes towards robocalls to mobile phones, TNS finds that 48% of wireline calls in 2021 were unwanted, compared to 21% to wireless numbers.

Distribution of Scoring for Wireline Telephone Numbers—2021

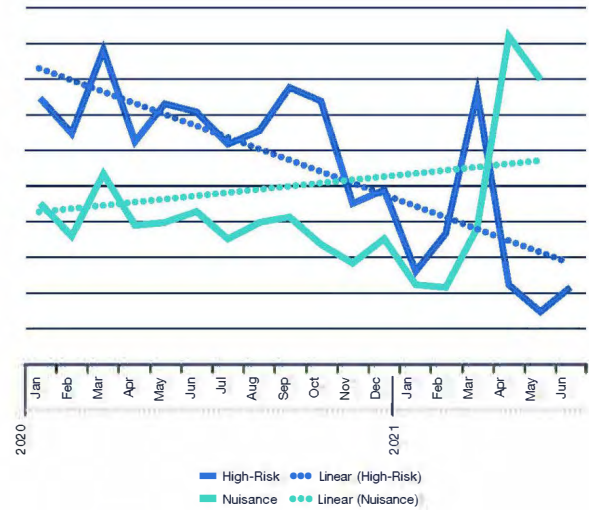


Unwanted calls to wireless numbers are only 21% of the total volume with high-risk and nuisance calls split evenly.

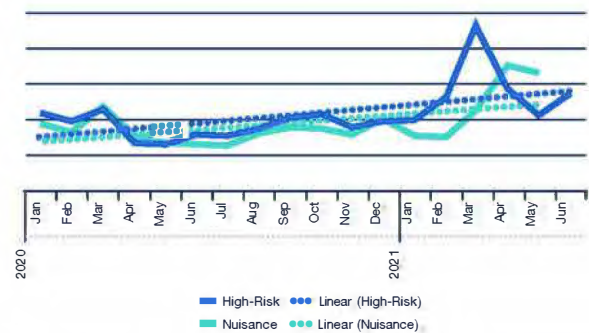
Distribution of Scoring for Wireless Telephone Numbers—2021



Wireline Unwanted Call Trend



Wireless Unwanted Call Trend



Almost 50% of the calls to wireline are unwanted



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

Both wireline and wireless high-risk calls declined in 2020 but the number of nuisance calls increased. Wireline nuisance calls increased 105% while wireline high-risk calls decreased 54% in 2021. At the same time, wireless nuisance calls increased 143% while high-risk calls decreased 22% in the period noted above. Again, the increases are skewed by the lockdown from COVID-19 in 2020.

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

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

The Consumer and Governmental Affairs Bureau released a Staff Report on the state of deployment of advanced methods and tools to eliminate illegal and unwanted calls. This section tries to highlight the efforts made by AT&T, Bandwidth, Charter, Comcast, Cox, Frontier, CenturyLink, TDS Telecom, T-Mobile, US Cellular, Verizon and Vonage, all of which offer free blocking services, often through a third-party analytics company.¹⁵



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

- AT&T Wireless offers *Call Protect* for free
- T-Mobile offers *Scam Shield*, which includes caller ID and several other features at no additional cost
- Verizon Wireless offers *Call Filter* for free and in September 2020, Verizon and Apple, partnering with TNS, provided a new *Silence Junk Callers* feature to Verizon Call Filter customers using iPhones. The feature is enabled by default to forward to voicemail all high and medium-risk spam calls

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

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

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

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

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

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

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

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

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

Opt-in subscriber services may be impacting bad actors



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

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

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

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

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

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

Top Scams

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

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

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

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

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

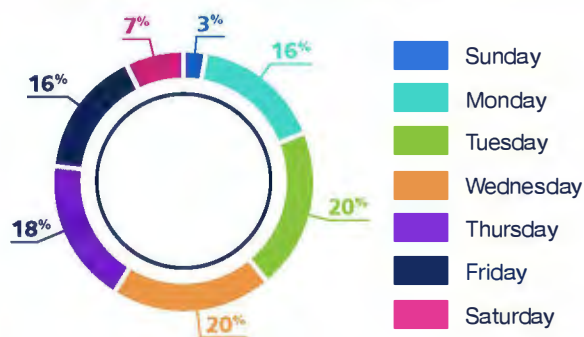
Home buying scam—The scams begin by asking what kind of property you own and if you are interested in selling it, attempting to make the call sound legitimate. Then they will make a bogus offer, possibly one you cannot refuse. The catch – there is an “administrative fee” which, after being paid, results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

Political scam—These scams take on three forms:

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

The number of unwanted calls varies daily but the highest volume of unwanted calls (20%) occurred on Tuesdays and Wednesdays during 2021. The weekend represented 10% of total calls, a slight decrease from 14% in 2020.

Distribution of All Unwanted Calls—2021



Donation scam had highest volume on heaviest day in 1H2021

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

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

Political Robocalls & Robotexts

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

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

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

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

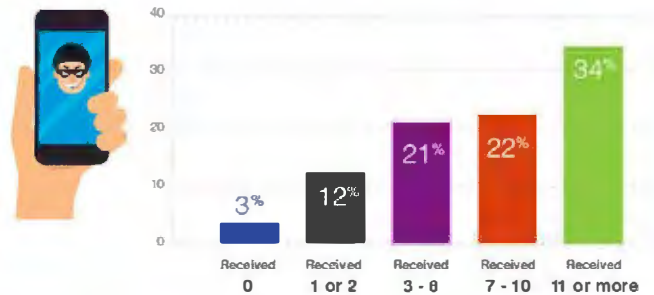
Senior Scams

A TNS survey in 1H2020 found that 53% of US senior citizens believe robocallers tried to scam them out of personal information in 2019; and nearly as many (47%) reported that they were targets of financial scams in 2018.²¹

Additional findings from the survey:

- **Robocall volume is high among seniors.** Almost 90% (89%) of seniors receive at least one robocall per week while more than half (56%) receive at least seven robocalls per week.
- **Seniors in dark about healthcare scams.** Even though 45% of seniors received a healthcare-related scam call, only 21% reported that they received information from their healthcare provider on robocall scams; this is problematic as older Americans are vulnerable to health scams fueled by the pandemic.

- **Seniors lack awareness of robocall filtering apps.** While 25% of respondents use a robocall blocking app from their carrier, two-thirds (66%) of seniors are not aware if their carrier offers such protection – suggesting an opportunity for carriers to broaden app branding and education efforts.



TNS conducted another survey in early 2021 year to understand the consumer frustration with robocalls.

- **Pandemic highlights need for Branded Calling.** Health agencies have struggled to reach Americans via phone with important COVID-19 vaccine and exposure information. A majority of respondents (63%) would answer a call if the logo of a brand they recognized was displayed.
- **Consumers are confused about robocall blocking and reporting options.** The good news is that 38% of consumers have a robocall blocking app through their carrier and 19% use an over-the-top app. The bad news: more than half (51%) of consumers do not even know if they have a robocall blocking app on their smartphone - pointing to a need for more market education that free tools are available through the carrier. At the same time, only 28% of respondents submitted a robocall complaint to their state attorney general, the FTC or the Do-Not-Call Registry.
- **Millennials are the most fed up with robocalls.** Millennials consistently outpaced other generations when it came to robocall frustration.
- **Robocalls to wireline home phones overlooked.** Overall, 78% of respondents, and 90% of 55-64-year-olds, believe robocalls to wireline phones are a growing but are an overlooked problem. And given that 57% of consumers said most calls to their home phone (if they have one) are robocalls, it is hardly a surprise that nearly three in 10 (29%) got rid of their wireline phone service because of robocalls.

- **Americans want robocall scammers to pay...with jail time.** Eighty-five percent (85%) believe robocallers who try to scam consumers should get jail time while 90% believe these robocalls should pay a financial penalty/fine. When asked who was responsible for stopping these calls, answers were mixed: the federal government (20%); my wireless/wireline carrier (18%); businesses trying to sell me products/services (9%); robocall blocking mobile app vendors (6%); my state government (5%); while 35% said all the above are responsible.

Neighbor Spoofing

As mentioned earlier, Neighbor Spoofing is a tactic bad actors use to trick consumers into answering their spam calls. To combat this, TNS launched its **Neighbor Spoofing** feature in mid-2018 and has continued to evolve it to protect consumers.

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

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

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

Typically, the numbers will have the same area code or local calling area to incite the consumer to answer. TNS has discovered such patterns and has proactively classified them as medium-risk.

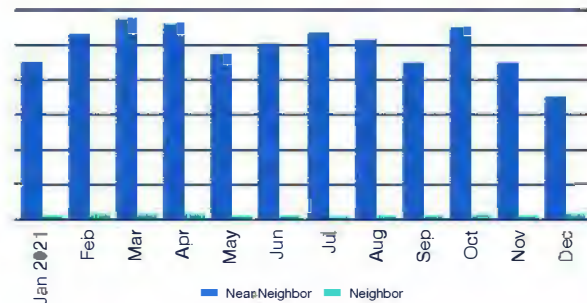
TNS has seen a small decline (-3%) in true neighbor spoofing, as bad actors are using neighbor spoofing less due to implementation of STIR/SHAKEN on the major wireless networks. Instead, they have shifted to near-neighbor spoofing where the area codes are the same, but not the first five or six digits. TNS has seen a remarkable increase of 64% in near-neighbor spoofing on a per subscriber basis.

Near-Neighbor Spoofing Events per Subscriber



In addition, the call volume from near-neighbor spoofing numbers or legitimate telephone numbers from VoIP providers is over 3,000 times the volume compared to “pure” neighbor spoofing where the area code and exchange are the same.

Neighbor Spoofing vs. Near-Neighbor Spoofing—2021



Near-neighbor spoofing continues to increase at over 60%



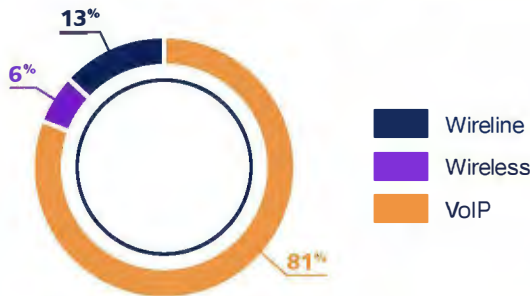
Snowshoe spamming is difficult to detect for over-the-top (OTT) applications. To be effective an application must be integrated with the network and see the cross-carrier events of both the calling number and the called number.

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

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

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

Near-Neighbor Spoofing by Line Type—2021



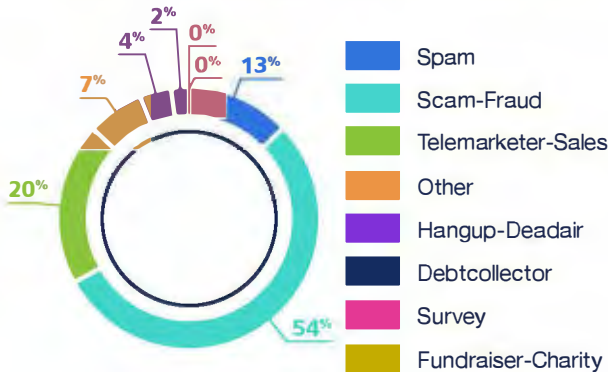
Crowd-Sourced Statistics

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

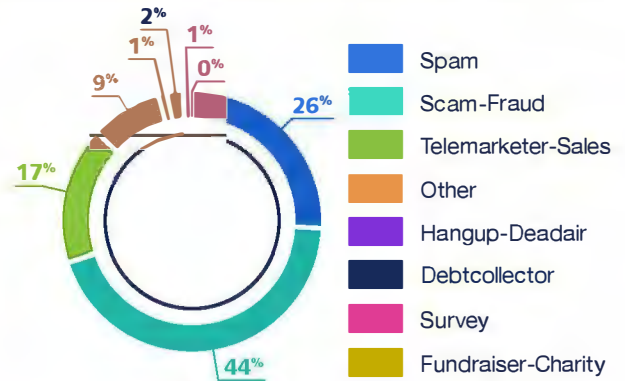
Enhanced Caller ID identifies callers or texters with their names displayed directly in the incoming call screen and message threads, even if their number is not in contacts.

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

Crowd-Source Feedback by Major Category—2021



Crowd-Sourced Feedback by Major Category—2020



When the end-users leave comments associated with unwanted calls, the top words used for all of 2021 are:

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



Looking at just the second half of the year, the word cloud looks like the following.



Auto Warranty Spamming

Many wireless subscribers have probably seen a local number calling them and not wanting to think they are missing an important call, hear a variation of the following:

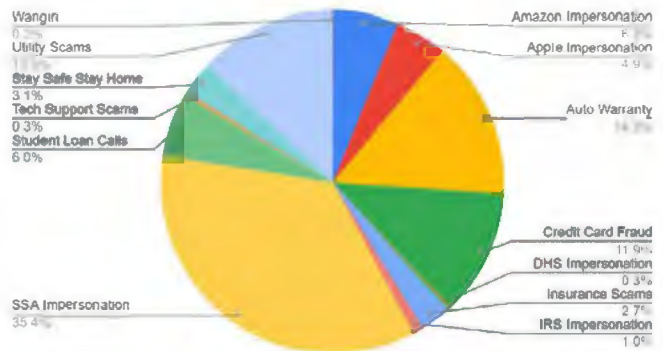
“Hi. This is Melanie. I’m giving you a call from the dealer service Center. We recently noticed your cars extended warranty would expire and wanted to provide you with one final courtesy call before your warranty expires and your warranty coverage becomes voided. This would make you financially responsible for all service repairs. If you wish to extend or reinstate your car’s warranty, Press four now.”

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

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

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

Active Campaigns 2021



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

Low-volume spamming techniques have grown more sophisticated



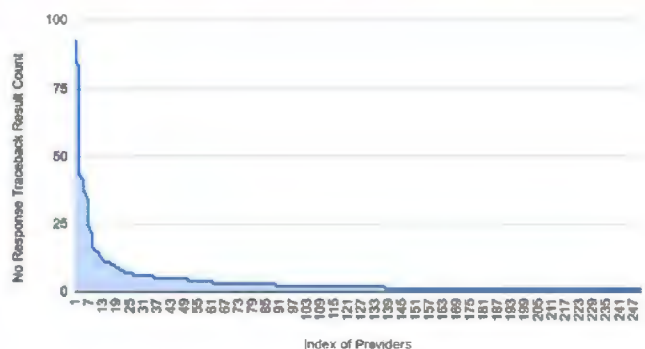
Report to Congress on Robocalls and Transmission of Misleading or Inaccurate Caller Identification Information

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



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

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



STIR/SHAKEN Attested Traffic

While STIR/SHAKEN cannot address an incoming call's intent, it does authenticate the calling number and is indisputably an essential foundational layer to combat spoofing. The FCC focused on larger voice service providers that have over 100,000 subscribers to implement STIR/SHAKEN by June 30, 2021.

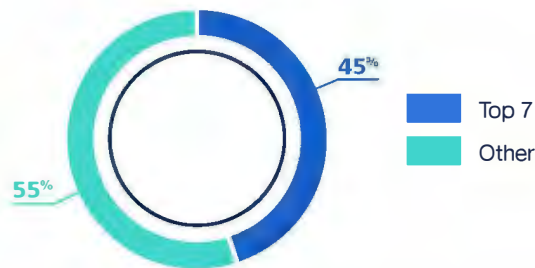
However, the amount of cross-carrier traffic between the seven largest US carriers (AT&T, CenturyLink, Charter, Comcast, T-Mobile, US Cellular and Verizon) account for less than half of the volume.

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

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

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

Cross-Carrier Traffic Among Tier-1 Carriers—2021

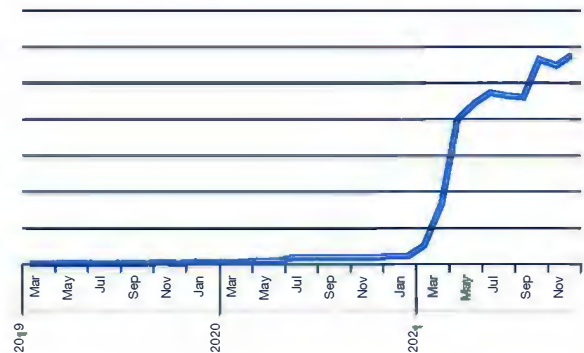


Partial Attestation (B)—The service provider has authenticated the call origination, but cannot verify the call source is authorized to use the calling number

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

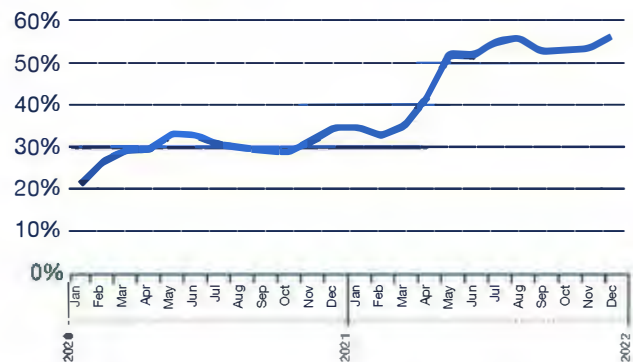
The amount of inter-carrier traffic that TNS has seen shows attestation has continued to grow dramatically in 1H2021.

Inter-Carrier Signed STIR/SHAKEN Traffic



- TNS estimates that call attestation has grown from 35% of the total traffic at the end of 2021 to over 56% by the end of 2021.

STIR/SHAKEN Traffic to Total Traffic



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

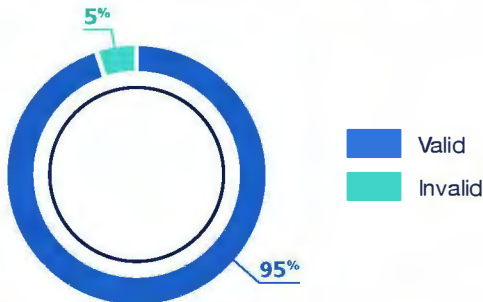


STIR/SHAKEN
needs to expand
beyond the Tier-1
providers to have a
significant impact

Invalid/Unallocated Number Use

The one constant in the robocall dilemma is that bad actors change tactics quickly. Using spoofed numbers is one of those tactics. Spoofing of invalid/unallocated numbers increased over 50% comparing 2021 to 2020. However, it is important to note that invalid/unallocated numbers remain a small percentage of total unwanted call volume at just 5%.

Unwanted Calls by Valid/Invalid NPA-NXX—2021



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

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

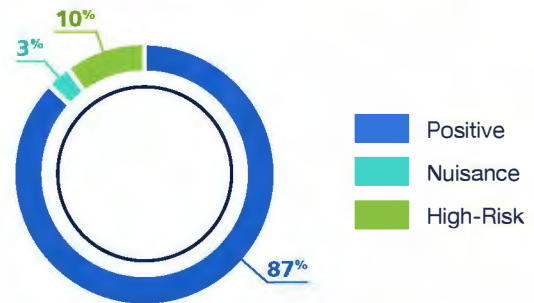
Canadian Results

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

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

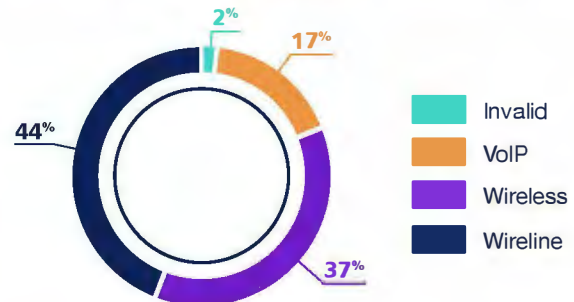
TNS found less than 20% of Canadian inter-carrier calls in 2021 were scored as unwanted, consistent with 2020 and 2019.

Scoring by Category Canadian Telephone Numbers—2021



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

Distribution of Unwanted Calls from Canadian Telephone Numbers—2021



International Results

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

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

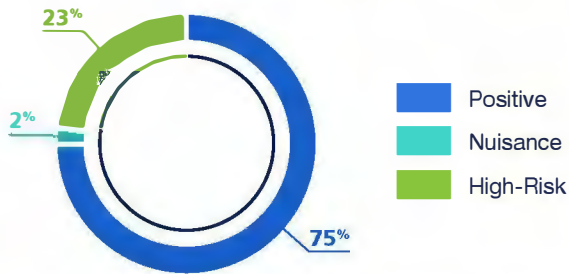
Many of the high-risk calls that come from international numbers are associated with **Wangiri** attacks.

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

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

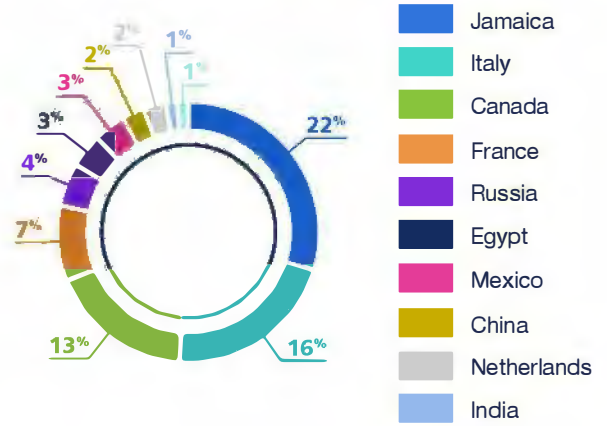
Every time you call, you will be charged high international rates or other connection fees. The bad actor profits from those fees.

Scoring by Category International Telephone Numbers—2021



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

Unwanted Calls from International Telephone Numbers—2021



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



How Carriers Should Address FCC Rule on Automatic Call Blocking

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

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

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

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

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

Recognize All Robocalls are Not Created Equal

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

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

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

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

At the same time, most consumers still want to utilize voicemail for call screening. Almost 70% of consumers want lower-risk calls sent to voicemail, letting them control which messages to return.²⁴ The takeaway for carriers, policymakers and regulators is that while consumers want protection from robocalls, they still want some control for less damaging nuisance calls.

It's All About Data Analytics

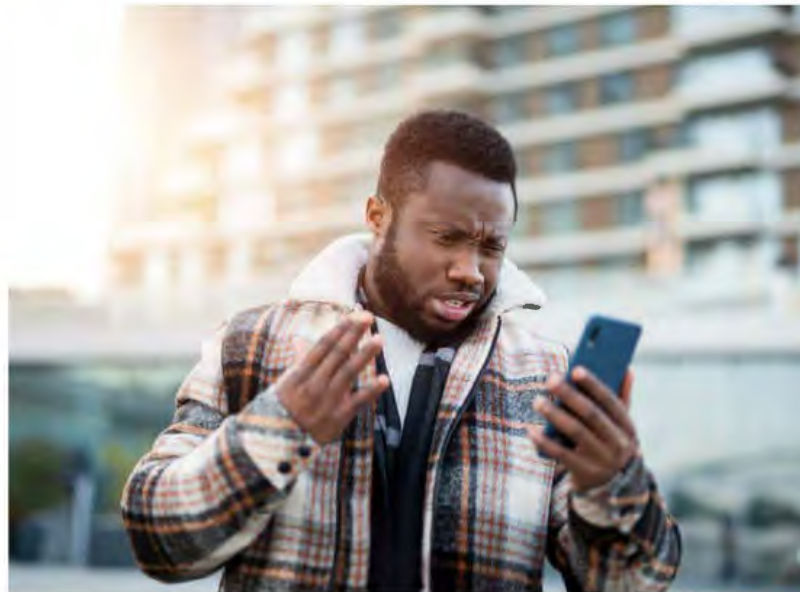
Without trust in the underlying data, it is impossible for consumers to feel comfortable in ceding control in call blocking. Today, it is already possible to detect caller ID spoofing and other malicious and nuisance robocalling behavior based on real-time network data analytics.

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

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

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

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



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.²⁵ Ironically, the same percentage is not aware that such an app is offered. This is a red flag for more aggressive consumer education regarding the availability of this service/technology and the benefits these apps provide.

Branded Calling When it Comes to STIR/SHAKEN is a Foundational Layer, not a Silver Bullet

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

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

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

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

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

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



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



How Can Call Originators Get Customers to Answer the Phone?

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

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

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

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

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

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

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

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

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

Don't Use One Main Calling Number for Multiple Uses

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

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

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

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

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



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

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

Provide a Consistent Calling Name Profile that Matches Context:

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

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

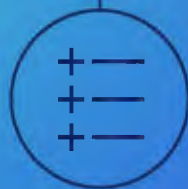
Document Normal Calling Patterns

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

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

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

Enterprises should work with analytics providers to register their calling campaigns



Don't Call Unassigned Numbers Frequently

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

Comply with DNC Lists, TCPA and FDCPA

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

Branded Calling

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

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

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

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

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

Branded Calling Study

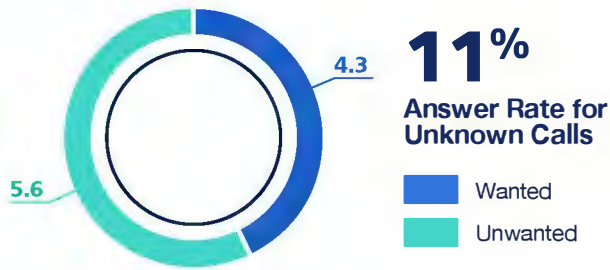
TNS conducted a study in 2021 to understand the trust and behavior associated with incoming calls from enterprises. The goal was to determine how users react when no information is available about a caller. The study provided a baseline of user sentiment of enterprise calls and user expectations of a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

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



Call verification is still misunderstood

Unknown Calls



Brand presence has strong effect on the consumer trust. A majority of consumers (52%) say that seeing the brand on the incoming call has a strong effect on their trusting the call.

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

The content delivered to the consumer influences trust.

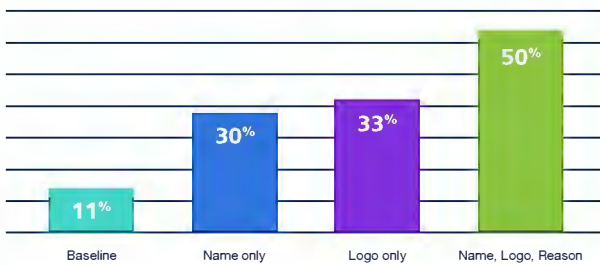
Consumers are five times more likely to answer a call with brand presence than a simple phone number.

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

Consumers Most Interested in Calls From



Percent Likely to Answer



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

Interpretations of "Caller Verified" Verstat



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

Experience with Caller ID/Caller Protection Services



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

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

FCC Releases Draft Version on Numbering Policy for Modern Communications

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

The **NPRM** would do the following:

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

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

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

The Third Report and Order:

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

FCC Adopted Two Robocall Items in their Open Meeting

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

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

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

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

<https://docs.fcc.gov/public/attachments/DOC-37103A1.pdf>

<https://docs.fcc.gov/public/attachments/DOC-37111A1.pdf>

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

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

<https://www.fcc.gov/document/fcc-proposes-largest-robocall-fine-until-tcpa>

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

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

Wireless Competition Bureau Seeks Comment on Two TRACED Act Obligations

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

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

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

The NPRM would:

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



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

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

FCC Adopts PSAP and Gateway Provider Robocall NPRMs

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

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

²⁹ <https://www.fcc.gov/document/fcc-keeps-industry-traceback-group-official-robocall-fighting-consortium>

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

³¹ <https://www.fcc.gov/document/shielding-illegal-calls-entering-911-call-centers>

³² <https://docs.fcc.gov/public/attachments/DOCS-376111A1.pdf>

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

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

Wireline Competition Bureau Adopts Protective Order for Robocall Mitigation Program Descriptions

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

Acting Chair Rosenworcel Proposes Rules to Combat Rise of Robotexts

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

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

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

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

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

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

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

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

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

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

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

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

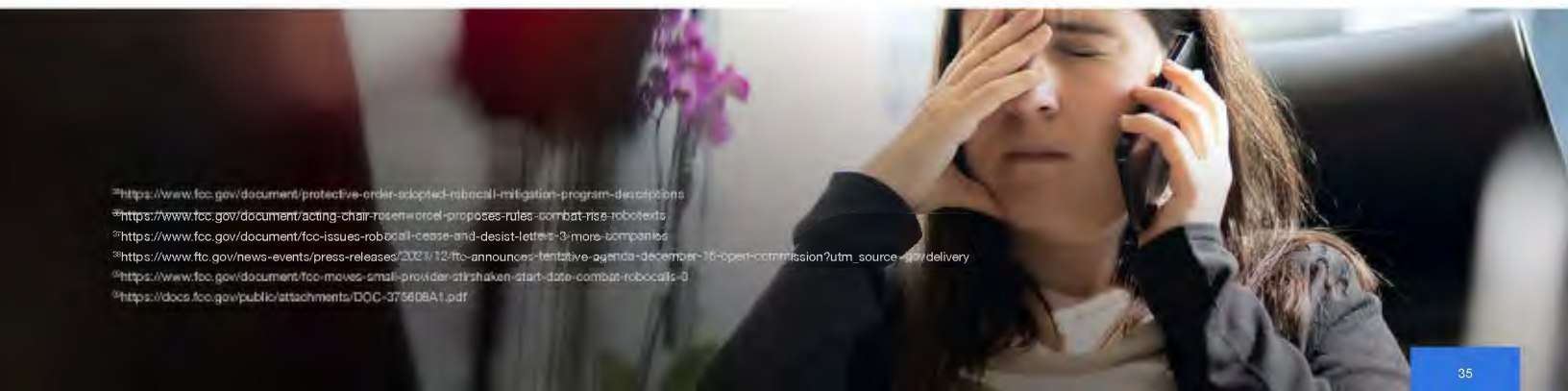
³⁶<https://www.fcc.gov/document/acting-chair-rosenworcel-proposes-rules-combat-rise-robotexts>

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

³⁸https://www.ftc.gov/news-events/press-releases/2021/12/ftc-announces-tentative-agenda-december-16-open-commission?utm_source=govdelivery

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

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



Industry Solutions to Combat Robocalling

Hardware and Software

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

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

Blacklists and Whitelists

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

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

Landline Call Blockers

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

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

Some models also can create a user-generated whitelist.⁴⁰

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.^{41 42}

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.⁴³

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.

⁴⁰ <http://www.consumer.ftc.gov/cro/magazine/2015/07/robocall-blocker-judew/index.html>

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

⁴² <http://www.ihackinnews.com/2013/07/truecaller-database-hacked-by-ryan.html>

⁴³ <http://apple.com/efwca/public/attachmatch/DA16-1121A1.pdf>

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

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

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

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

Real-Time Analytics

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

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

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

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

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

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

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

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

Enterprise Response to Analytics

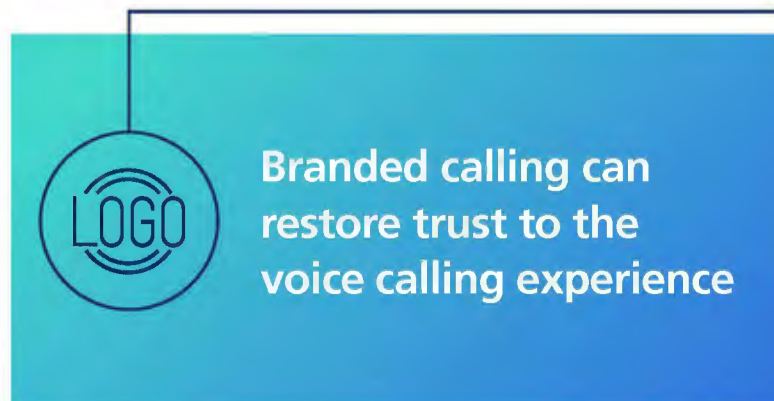
TNS has observed a varied response among enterprises to the mitigation techniques that the industry has employed. Among the good actors, there has been a general willingness to adapt methodologies to conform with the analytics tools' definitions of good behavior.

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

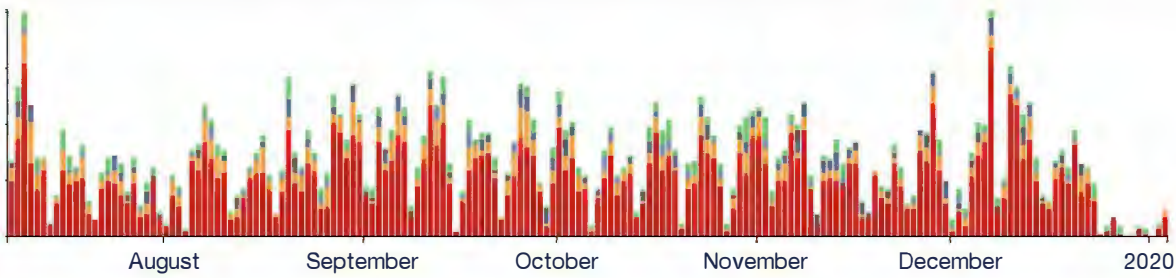
Further, products that provide call origination aggregators and enterprises with a view into their call centers' practices, such as **Telephone Number Reputation Monitoring** from TNS, allow them to understand how their numbers are being characterized, and when activity triggers unwanted reputational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

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

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

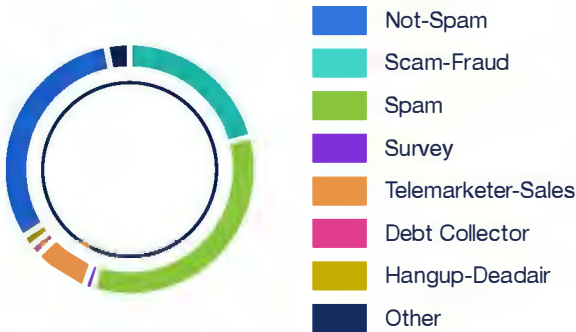


Branded calling can restore trust to the voice calling experience



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.

Category Distribution




The FCC and CRTC continue exploration of methods to counter bad actors including blocking, adopting protocols to prevent number spoofing and tracebacks. They have reached out to the service providers seeking the industry's help in their latest public notices to refresh the record on advanced methods to target and eliminate unlawful robocalls.

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

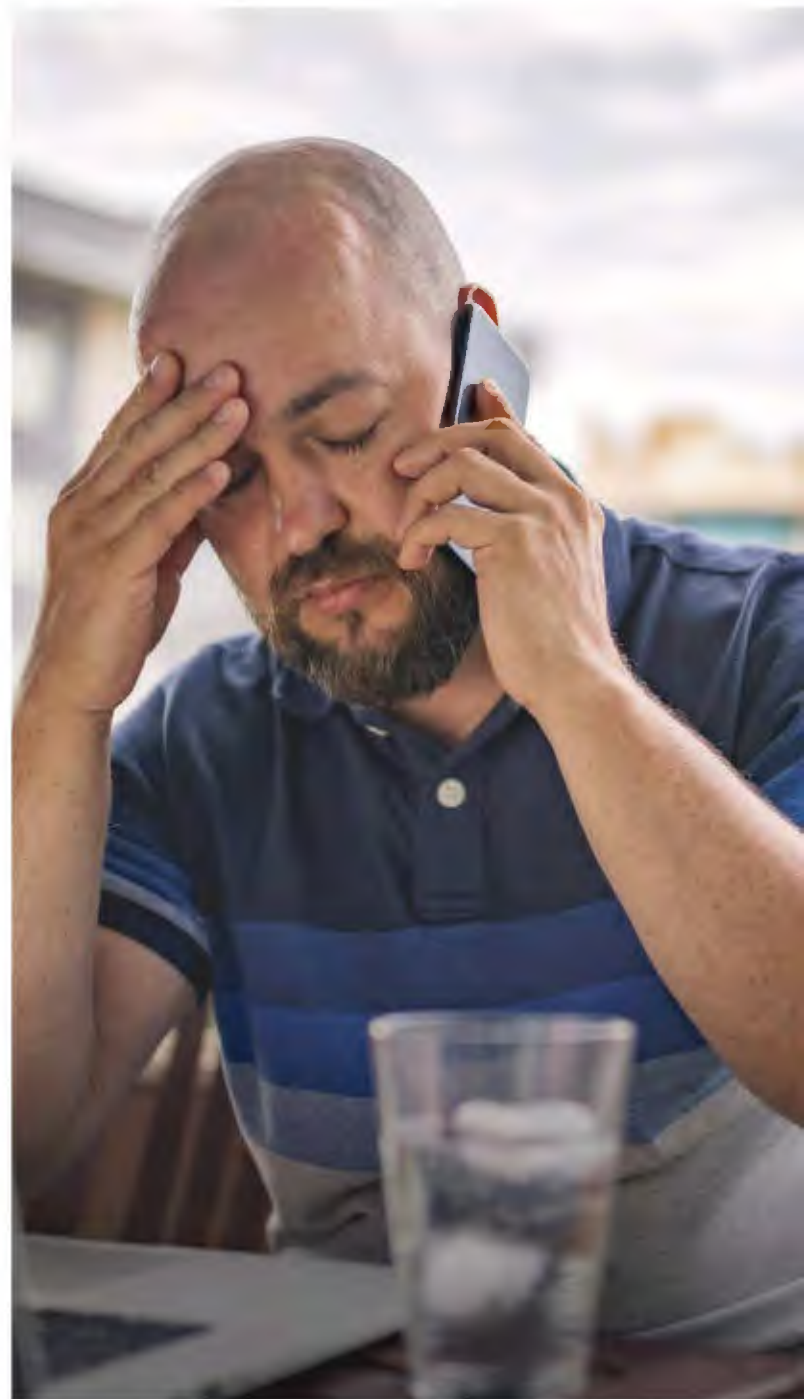
In addition, analytics providers will be explaining the complex role they play in solving this on-going scourge.

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

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

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

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



A layered approach is most effective in combating robocalls



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

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

ITG - High-Volume Robocall Campaign Origination Analysis - Domestic Origination

Rank	total count	sum(isUsOrig)	Provider	Form 499	RMD
1	67	57	PZ / Illum Telecommunication	interconnected VoIP	RMD0002232
2	50	50	Yodel Technologies / Yodel Voice	interconnected VoIP	none
3	35	35	Duratel	interconnected VoIP	RMD0001951
4	32	32	Prestige DR Voip	Non-interconnected VoIP	none
5	30	30	Primo Dialler	interconnected VoIP	RMD0001592
6	24	24	Mak Links Corp	interconnected VoIP	RMD0001592
7	20	17	BestiumPro	interconnected VoIP	none
8	17	17	VaultTel Solutions	interconnected VoIP	RMD0001716
9	16	16	Inteliquent / Onvoy / Vitelity / Neutral Tandem	CAP/LEC	yes (several entries)
10	12	12	VoIP Essential / Rapid Eagle	interconnected VoIP	RMD0001639
11	11	11	Andopcall	none	none
12	11	10	FIMAC Inc.	none	none
13	11	10	System Global	none	none
14	10	10	Range Telecom	interconnected VoIP	RMD0001995
15	10	10	Tellza / Phonetime / Matchcom	Other Toll	RMD0003760
16	10	10	Zcom solutions	none	none
17	9	9	Apex Telecom LLC	interconnected VoIP	RMD0004223
18	8	8	Dynamic Interactive / Call Tools	interconnected VoIP	RMD0004739
19	9	7	Ytel	Toll Reseller	RMD0001412
20	6	6	Bare Telecom LLC	interconnected VoIP	RMD0002230
21	6	6	Magnify Telecom / Just Deliver It	none	none
22	6	6	Netlatitude Inc.	none	none
23	7	2	Hello Hello Miami, LLC	Non-interconnected VoIP	RMD0005460

ITG - High-Volume Robocall Campaign Origination Analysis - Foreign Origination

Rank	count	m(isNonUsOr	Provider	Country	Form 499	RMD
1	62	62	Fortress Leads S DE RL DE CV	Meixco	none	RMD0004908
2	19	18	Axkan Consultores	Mexico	non-interconnected VoIP	RMD0007384
3	21	16	Insync Voice	Phillippines	none	RMD0005215
4	14	14	TMO GROUP/TheMyOperator	United Kingdom	none	none
5	9	9	Telecom Unlimited	Mexico	none*	none
6	9	8	Paakc	Pakistan	none	none
7	8	8	VoxPace	Singapore	none	none
8	7	7	Mash Telecom	Canada	internetconnected VoIP	RMD0001613
9	6	6	VoIPMEN Pvt Ltd / Dialer360	Pakistan	none	none
10	8	5	Clevertel	Hong Kong	none	RMD0005114
11	7	5	Elysian Telecom	Hong Kong	none	none
12	7	4	CHINA SKYLINE TELECOM CO LTD	Hong Kong	none	none
13	8	1	Lexico Telecom LTD	Latvia	none	none

*There is a U.S.-based Telecom Unlimited but it appears to be a different entity. The Telecom Unlimited in our system is reportedly based in Mexico; the Form 499 filer in Texas. We also have a email address domain that does not match the one in the Form 499, though it's possible we were provided an email with a typo.

ITG - High-Volume Robocall Campaign Origination Analysis - Non-Responsive

Rank	Count	Provider	Country	Form 499	RMD
1	57	Fugle Telecom LLC	United States	CAP/LEC	none
2	57	Sumco	Panama	none	none
3	15	Voizbiz Information Technology Solutions	Phillipines	interconnected VoIP	none
4	13	Laxmi Networks / LMC Networks	India	none	none
5	12	Geist Telecom	United States	interconnected VoIP	none
6	11	Marketing Maestros	Pakistan	none	none
7	10	PZ / Illum Telecommunication	United States	interconnected VoIP	RMD0002232
8	9	Global Bridge Communications / GBC	India	none	none
9	9	Vitcomm	United States	none	none
10	7	Nexcess Telecom Ltd	UAE	none	none
11	7	Teraz Telecom	United States	private service provider	RMD0003467
12	7	VODAFONE US	United States	CAP/LEC	RMD0004671
13	7	Lexico Telecom LTD	Latvia	none	none
14	6	Kosmos Communications	United States	none	none
15	6	NGT Networks Pte. Ltd	Singapore	none	none
16	6	Xicomm LLC	United States	non-interconnected VoIP	RMD0001280

ITG - High-Volume Robocall Campaign Origination Analysis - 6 month-Providers-by-origin-nonr

total count	sum(isNonResponsive)	sum(isUsOrig)	sum(isNonUsOrig)	Provider	Min	Max
50	0	50	0	Yodel Technologies / Yodel Voice	2021-03	2021-05
35	0	35	0	Duratel	2021-04	2021-08
32	0	32	0	Prestige DR Voip	2021-03	2021-07
30	0	30	0	Primo Dialler	2021-05	2021-07
24	0	24	0	Mak Links Corp	2021-03	2021-07
17	0	17	0	VaultTel Solutions	2021-03	2021-08
16	0	16	0	Inteliquent / Onvoy / Vitelity / Neutral Tandem	2021-04	2021-08
12	0	12	0	VoIP Essential / Rapid Eagle	2021-06	2021-07
11	0	11	0	Andopcall	2021-07	2021-07
10	0	10	0	Range Telecom	2021-07	2021-08
10	0	10	0	Tellza / Phonetime / Matchcom	2021-03	2021-05
10	0	10	0	Zcom solutions	2021-05	2021-05
9	0	9	0	Apex Telecom LLC	2021-03	2021-08
8	0	8	0	Dynamic Interactive / Call Tools	2021-03	2021-04
6	0	6	0	Bare Telecom LLC	2021-03	2021-04
6	0	6	0	Magnify Telecom / Just Deliver It	2021-03	2021-03
6	0	6	0	Netlatitude Inc.	2021-04	2021-04
62	0	0	62	Fortress Leads S DE RL DE CV	2021-04	2021-08
14	0	0	14	TMO GROUP/TheMyOperator	2021-07	2021-08
9	0	0	9	Telecom Unlimited	2021-05	2021-08
8	0	0	8	VoxPace	2021-03	2021-08
7	0	0	7	Mash Telecom	2021-03	2021-03
6	0	0	6	VoIPMEN Pvt Ltd / Dialer360	2021-03	2021-03
11	1	10	0	FIMAC Inc.	2021-06	2021-06
11	1	10	0	System Global	2021-03	2021-04
19	1	0	18	Axkan Consultores	2021-03	2021-08
9	1	0	8	Paakc	2021-04	2021-08
9	2	7	0	Ytel	2021-04	2021-06
7	2	0	5	Elysian Telecom	2021-03	2021-06

ITG - High-Volume Robocall Campaign Origination Analysis - 6 month-Providers-by-origin-nonr

total count	sum(isNonResponsive)	sum(isUsOrig)	sum(isNonUsOrig)	Provider	Min	Max
20	3	17	0	BestiumPro	2021-03	2021-06
8	3	0	5	Clevertel	2021-08	2021-08
7	3	0	4	CHINA SKYLINE TELECOM CO LTD	2021-03	2021-06
21	5	16	0	Insync Voice	2021-03	2021-08
7	5	2	0	Hello Hello Miami, LLC	2021-06	2021-07
6	6	0	0	Kosmos Communications	2021-08	2021-08
6	6	0	0	NGT Networks Pte. Ltd	2021-06	2021-06
6	6	0	0	Xicomm LLC	2021-06	2021-08
8	7	0	1	Lexico Telecom LTD	2021-03	2021-08
7	7	0	0	Nexcess Telecom Ltd	2021-04	2021-06
7	7	0	0	Teraz Telecom	2021-03	2021-06
7	7	0	0	VODAFONE US	2021-04	2021-07
9	9	0	0	Global Bridge Communications / GBC	2021-08	2021-08
9	9	0	0	Vitcomm	2021-03	2021-04
67	10	57	0	PZ / Illum Telecommunication	2021-03	2021-08
11	11	0	0	Marketing Maestros	2021-03	2021-08
12	12	0	0	Geist Telecom	2021-06	2021-08
13	13	0	0	Laxmi Networks / LMC Networks	2021-03	2021-07
15	15	0	0	Voizbiz Information Technology Solutions	2021-04	2021-06
57	57	0	0	Fugle Telecom LLC	2021-04	2021-08
57	57	0	0	Sumco	2021-03	2021-08

Industry Traceback Group:

High-Volume Robocall Campaign Origination Analysis



Query Parameters

- 6-month period
- Limited to high-volume robocall campaigns
- Includes providers that appeared in at least five total tracebacks

Query Results

- 824 total tracebacks
 - 395 identified domestic originator*
 - 163 identified foreign originator
 - 222 concluded with non-responsive providers
 - 44 concluded without response from providers that typically respond
- Providers
 - 23 domestic originators*
 - 13 foreign originators
 - 14 non-responsive providers

*Six purportedly domestic providers did not file in the Form 499 database nor RMD

Top Domestic Originators

Rank	Count	Provider	Form 499 Categorization	RMD Filing
1	57 (+10 NR)	PZ / Illum Telecommunication	Interconnected VoIP	Yes
2	50	Yodel Technologies	Interconnected VoIP	No
3	35	Duratel	Interconnected VoIP	Yes
4	32	Prestige DR Voip	Non-interconnected VoIP	No
5	30	Primo Dialler	Interconnected VoIP	Yes
6	24	Mak Links Corp	Interconnected VoIP	Yes
7	17 (+3 NR)	BestiumPro	Interconnected VoIP	No
7	17	VaultTel Solutions	Interconnected VoIP	Yes
9	16	Inteliquent / Onvoy / Vitelity / Neutral Tandem	CAP/LEC	Yes
10	12	VoIP Essential / Rapid Eagle	Interconnected VoIP	Yes

Domestic Originators Summary

- Top Heavy-Distribution
 - Top 8 are VoIP, and 9 of top 10
 - Top 8 identified as the originator in 262 tracebacks, 66% of query results
 - 84% of all domestically-originated calls traced back from providers identified as originator in 4+ tracebacks
- Total
 - 23 providers with 5+ tracebacks
 - 14 are VoIP providers (12 interconnected, 2 non-interconnected)
 - 1 CAP/LEC
 - 2 identified as toll (1 other toll, 1 toll reseller)
 - 6 claim to be U.S.-based but lack Form 499 and RMD filings

Top Foreign Originators

Rank	Count	Provider	Form 499 Categorization	RMD Filing
1	62	Fortress Leads S DE RL DE CV (MX)	None	Yes
2	18 (+1 NR)	Axkan Consultores (MX)	Non-interconnected VoIP	Yes
3	16 (+5 NR)	Insync Voice (RP)	None	Yes
4	14	TMO GROUP/TheMyOperator (UK)	None	No
5	9	Telecom Unlimited (MX)	None*	No
6	8	Paakc (PK)	None	No
6	8	VoxPace (SG)	None	No
8	7	Mash Telecom (CA)	Interconnected VoIP	Yes
9	6	VoIPMEN Pvt Ltd / Dialer360 (PK)	None	No
10	5 (+3 NR)	Clevertel (HK)	None	Yes
10	5	Elysian Telecom (HK)	None	No



Foreign Originators Summary

- Still Top-Heavy but Broader Distribution Compared to Domestic
 - 65% of all foreign-originated calls traced back from providers identified as originator in 4+ tracebacks (excluding non-responsive)
- Total
 - 13 providers with 5+ tracebacks
 - Likely all VoIP providers based on ITG information and belief
 - Only 2* in Form 499 Filer Database and only 5 in RMD

Top Non-Responsive

Rank	Count	Provider	Form 499 Categorization	RMD Filing
1	57	Fugle Telecom LLC (US)	CAP/LEC	No
1	57	Sumco (PA)	None	No
3	15	Voizbiz Information Technology Solutions (RP)	Interconnected VoIP	No
4	13	Laxmi Networks / LMC Networks (IN)	None	No
5	12	Geist Telecom (US)	Interconnected VoIP	No
6	11	Marketing Maestros (PK)	None	No
7	10	PZ / Illum Telecommunication (US)	Interconnected VoIP	Yes
8	9	Global Bridge Communications / GBC (IN)	None	No
9	9	Vitcomm (US)	None	No
10	7	Lexico Telecom LTD (LV)	None	No
10	7	Nexcess Telecom Ltd (AE)	None	No
10	7	Teraz Telecom (US)	Private service provider	Intermediate
10	7	VODAFONE US (US)	CAP/LEC	Yes

Non-Responsive Summary

- Total
 - 18 providers did not respond to at least 5 tracebacks of which 14 did not respond to any tracebacks
 - 2 identified as CAP/LEC (*But see next slide....*)
 - 1 identified as private service provider
 - 5 identified as VoIP (3 interconnected, 2 non-interconnected)
 - 10 remaining have not submitted Form 499s

Non-Responsive Summary – Fugle Telecom LLC

Filer Identification Information:

499 Filer ID Number: **834185**
Registration Current as of:
Legal Name of Reporting Entity: **Fugle Telecom LLC**
Doing Business As:
Principal Communications Type: **CAP/LEC**
Universal Service Fund Contributor: **No**
(Contact USAC at 888-641-8722 if this is not correct.)
Holding Company:
Registration Number (CORESID):
Management Company:
Headquarters Address:
City:
State:
ZIP Code:
Customer Inquiries Address:
City:
State:
ZIP Code:
Customer Inquiries Telephone:
Other Trade Names:

Agent for Service of Process:

Local/Alternate Agent for Service of Process:
Telephone:
Extension:
Fax:
E-mail:
Business Address of Agent for Mail or Hand Service of Documents:
City:
State:
ZIP Code:
D.C. Agent for Service of Process:
Telephone:
Extension:
Fax:
E-Mail:
Business Address of D.C. Agent for Mail or Hand Service of Documents:
City:
State:
ZIP Code:

FCC Registration Information:

Chief Executive Officer:
Business Address:
City:
State:
ZIP Code:
Chairman or Other Senior Officer:
Business Address:
City:
State:
ZIP Code:
President or Other Senior Officer:
Business Address:
City:
State:
ZIP Code:
Jurisdictions in Which the Filing Entity