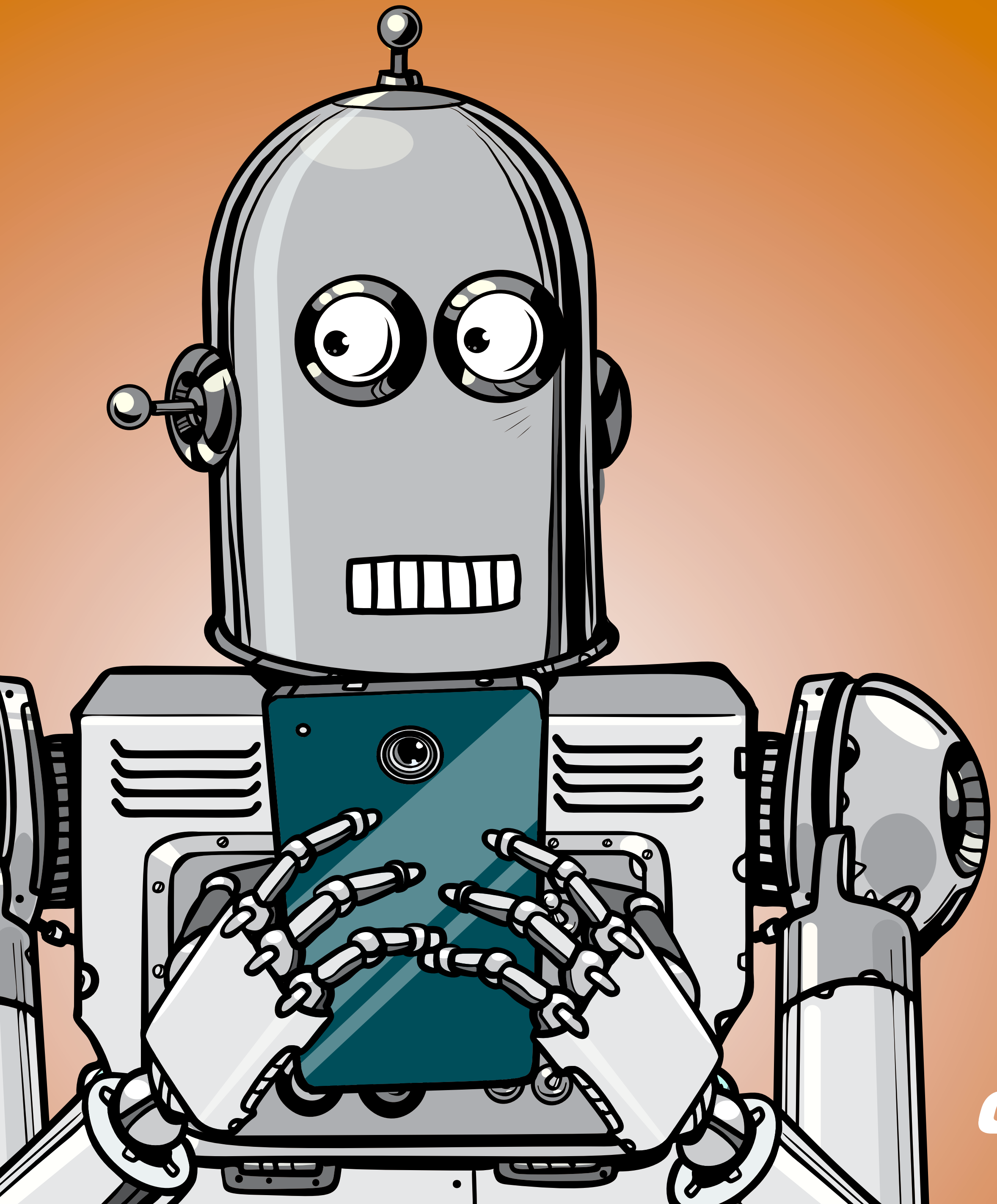
ROBOCALLING AND COMMUNICATION ID SPOOFING:

Better Understanding Illicit and Unwanted Calls and How to Counter Them

February 2021



ABSTRACT

It is well recognized within the telecommunications industry that illicit and nuisance calling, specifically illegal scam robocalls, has led to a significant loss of customer trust in the global telephone network. To restore this trust, carriers and service providers (SPs) have gone to considerable lengths to design and deploy services that will mitigate the impacts of these illicit calling campaigns.

This report aims to provide a detailed summary of both the many types of illicit calling and the measures being deployed to counter them. It explains why there is no "silver bullet" that will instantly and forever eliminate all illicit robocalling and why, instead, the industry must deploy many separate components in combination to maximize mitigation with minimal blocking of wanted calls. A summary is included of the various U.S. actions and some international regulators to assist carriers and SPs in this effort.

As these bad actors continue to evolve their techniques, further countermeasures will need to be developed to cope with these new threats. Accordingly, this report concludes with recommendations for future action by the Alliance for Telecommunications Industry Solutions (ATIS) and other organizations.

FOREWORD

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the all-internet protocol (IP) transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open-source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding partner of the oneM2M global initiative, a member of and major U.S. contributor to the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

NOTICE OF DISCLAIMER AND LIMITATION OF LIABILITY

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this document may require use of an invention covered by patent rights. By publication of this document, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to https://www.atis.org/policy/patent-policy/ for more information.

COPYRIGHT INFORMATION

ATIS-I-0000081

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005, USA

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

1

EXECUTIVE SUMMARY

EXECUTIVE SUMMARY

It is well recognized within the telecommunications industry that illicit and nuisance calling — specifically illegal scam robocalls — has led to a significant loss of customer trust in the global telephone network. In fact, eight-in-ten Americans say they do not generally answer their cellphone when an unknown number calls.[1] To restore this trust, carriers and service providers (SPs) have gone to considerable lengths to design and deploy services that will mitigate the impacts of these illicit calling campaigns.

This report aims to provide a detailed summary of both the many types of illicit calling and the measures being deployed to counter them. Many types of bad players generate these calls. This report explains why so many different types of fraud are perpetrated and describes the multiple techniques required to address them. There is no specific solution that will, on its own, stop all malicious use of false or misleading call identification.

Most carriers and many independent providers have call blocking and call information reporting services. Yet many questions remain about how these are provided and why, for example, they sometimes fail to eliminate all illicit calls. This report answers those questions by describing the various anti-robocalling techniques and how they work together to provide mitigation services.

It is important to remember that there are also legitimate and necessary uses of robocalling and ID spoofing, such as delivery of emergency information services. This report discusses how illicit calls and countermeasures affect legal calls.

One issue that has caused some confusion both within and outside the industry is the role and importance of some mitigation techniques that have gained high visibility. This report explains why there is no "silver bullet" that will instantly and forever eliminate all illicit robocalling and why, instead, the industry must deploy many separate components in combination to maximize mitigation with minimal blocking of wanted calls. This discussion includes techniques to verify the accuracy and ownership of calling numbers, and the problem of providing accurate calling name information and displaying it to the call recipient.

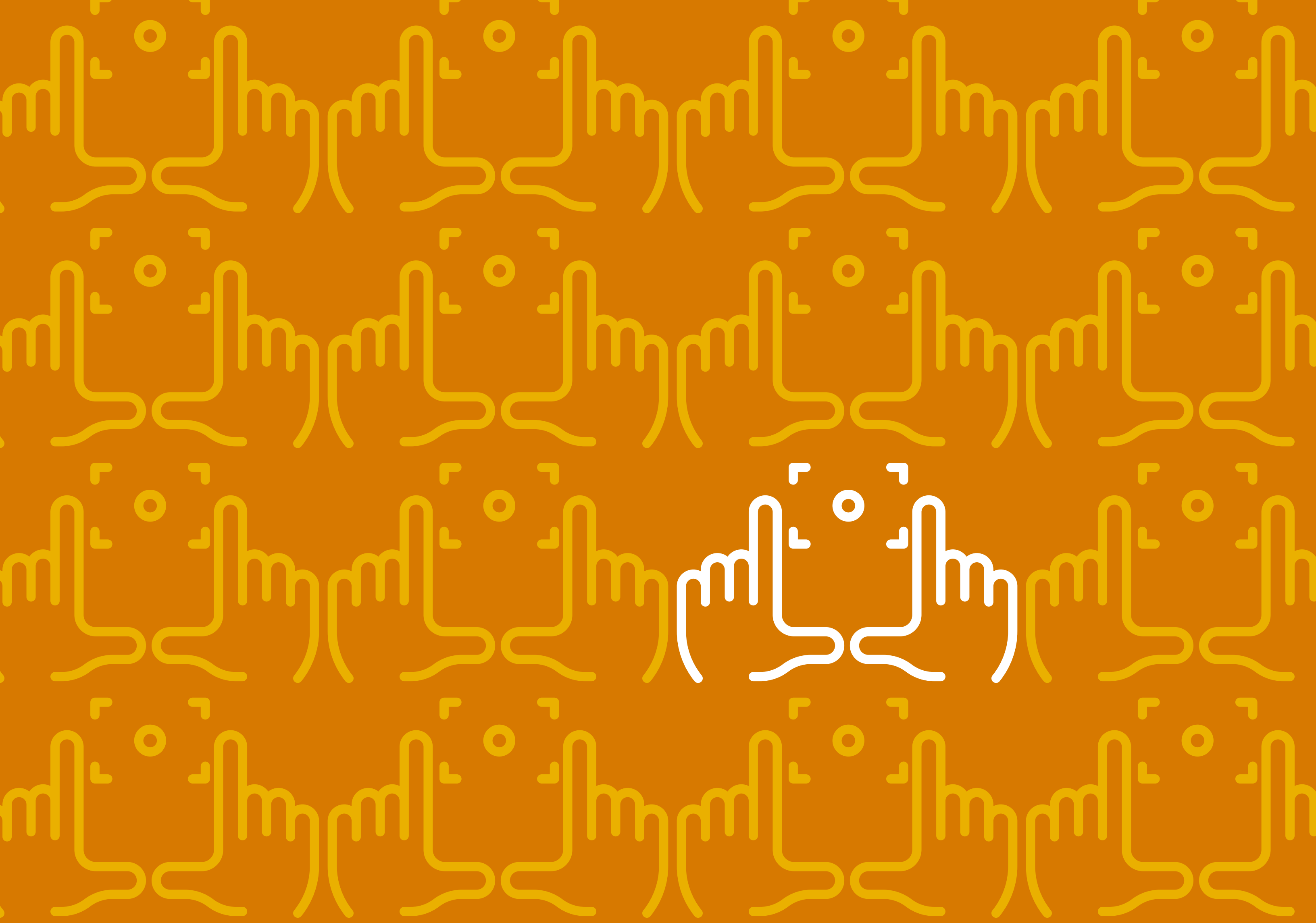
A summary is provided of actions by the U.S. and some international regulators to assist carriers and SPs in this effort.

Note that the term "mitigate" has been used throughout this report rather than "eliminate." One unfortunate fact is that as more and varied methods are deployed to counter these calls, perpetrators will continue to evolve their techniques to deliver calls with illicit content in ways that evade the countermeasures. As bad actors continue to evolve their techniques, further countermeasures will need to be developed to cope with new threats. The report provides recommendations for future action by the Alliance for Telecommunications Industry Solutions (ATIS) and other organizations.

Unfortunately, it is unlikely that the nuisance of illicit robocalls will ever be eliminated; this report should be periodically updated to reflect changes in threats and mitigation techniques.

Readers should note that this report has been compiled from many subject matter experts' contributions. Therefore, each section's writing style, and the order of material within those sections, have been optimized by the contributors for presentation of that specific content.

[1] Pew Research Center, "Most Americans Don't Answer Cellphone Calls from Unknown Numbers," December 14, 2020, https://www.pewresearch.org/fact-tank/2020/12/14/most-americans-dont-answer-cellphone-calls-from-unknown-numbers/.



2

INTRODUCTION AND SCOPE

INTRODUCTION

For many years, illicit robocalling has been the primary cause of consumer complaints to the Federal Communications Commission (FCC) and Federal Trade Commission (FTC). The scale of the problem is significant. October 2019 averaged over 182 million robocalls per day alone,[2] leading to a record 10,000 robocall complaints per day to the FTC.[3] It should be noted that robocalls declined by about 20% during the first six months of 2020. The annual total fell from nearly 58 billion robocalls in 2019 to 46 billion in 2020 even as call volumes grew since the start of the COVID-19 pandemic.[4] The FTC has also reported that the amount of robocall complaints it received was down 68% in April 2020 from April 2019 and down 60% in May 2020 compared to May 2019.[5] [6] Some of the robocall decline may correspond with call center shutdowns due to shelter-in-place measures taken to combat the pandemic. The FCC and the FTC also sent joint letters to gateway providers, warning against routing and transmitting illegal coronavirus-related scam robocalls.[7]

Robocalling is of interest to a wide range of parties, including consumers, carriers, and regulators. However, it also clearly impacts legitimate bulk callers and automated call centers, whose communications are now often lumped in with the illicit callers and rejected by consumers even before they are answered. When consumers allow legitimate calls to go straight to voicemail, those businesses incur costs related to follow-up calls and phone tag.

Many activities have been initiated to counter this robocalling threat, primarily to create and implement new technical standards and operational procedures. ATIS has previously provided summaries of these various activities and their impacts for internal planning purposes. This work builds on those activities to help the industry coordinate mitigation initiatives and provide a broad, current overview of those ongoing activities to combat illicit robocalling. It will address the use of different mitigation techniques and their combined use.

SCOPE

This report provides an overview of the activities designed to produce and implement measures to mitigate both the scourge of illicit robocalling and the falsification of originating party identities that support it. This report begins by defining the real problems to be solved: specifically, how this impacts the choice and prioritization of mitigation solutions.

The report provides a single reference source that describes the various mitigation activities and points to more detailed sources of information about each one. It also discusses how these various techniques are used in combination to optimize mitigation, and how they impact and are impacted by the supporting regulatory and enforcement activities.

This report also examines parallel activities to mitigate illicit messaging spam with characteristics common with robocalling, such as Short Message Service (SMS) spamming, which shares a common address space.

Illegal spoofing and robocalling originate in many other regions rather than only North America, so this report also discusses global activities.

Finally, this report outlines opportunities for additional work by ATIS and other groups to enhance the current work on illicit robocalling mitigation. It also examines how this work can create opportunities for further commercial investment in technology to re-establish trust in the telecommunications network.

Note that in the U.S., illicit robocalling mitigation efforts have focused on helping recipients of these bad calls. This report reflects that emphasis. However, in other regions, the impact of similar illicit activity, notably ID spoofing, has also been felt by network operators because it directly impacts their revenues.[8] This report does not explicitly address that issue.

The major issue the industry confronts is the loss of consumer trust in telephony networks to deliver useful voice and SMS services. Because illicit callers spoof caller ID, many customers cannot distinguish between legitimate calls and those from illegal robocallers.

For this trust to be restored, the telecommunications industry and its regulators need access to tools that will eliminate or substantially reduce delivery of such calls or, at very least, warn recipients that a call may have bad intent.

[2] YouMail, “Record-Smashing 5.7 Billion Robocalls in October, Says YouMail Robocall Index,” CISION PR Newswire, November 5, 2019, https://www.prnewswire.com/news-releases/record-smashing-5-7-billion-robocalls-in-october-says-youmail-robocall-index-300951661.html.

[3] Room, Tony, “Crackdown Targets Robocallers that Placed 1 Billion Calls, Federal and State Officials Say,” Washington Post, June 25, 2019, https://www.washingtonpost.com/technology/2019/06/25/federal-state-officials-announce-enforcement-efforts-targeting-billion-illegal-robocalls/.

[4] YouMail, “Have Robocalls Taken Over the Phone Call?” YouMail Blog, July 21, 2020, https://blog.youmail.com/2020/07/have-robocalls-taken-over-the-phone-call/.

[5] Greisman, Lois, “Robocall Reports Still Down, FTC Still Fighting,” FTC Consumer Information, June 15, 2020, https://www.consumer.ftc.gov/blog/2020/06/robocall-reports-still-down-ftc-still-fighting.

[6] Federal Trade Commission, “Do Not Call Complaints,” October 2016-September 2020, https://public.tableau.com/profile/federal.trade.commission#!/vizhome/DoNotCallComplaints/Robocalls.

[7] Federal Trade Commission, “FTC and FCC Send Joint Letters to Additional VoIP Providers Warning against ‘Routing and Transmitting’ Illegal Coronavirus-related Robocalls,” Press Release, May 20, 2020, https://www.ftc.gov/news-events/press-releases/2020/05/ftc-fcc-send-joint-letters-additional-voip-providers-warning.

[8] I3 Forum, Technical Report: Calling Line Identification (CLI) Spoofing, Release 1.0, October 2020, http://i3forum.org/blog/2020/11/04/i3forum-calling-line-identification-cli-spoofing-report/.

3

PROBLEM DEFINITION AND SOLUTION OUTLINE

PROBLEM DEFINITION AND SOLUTION OUTLINE

Illicit robocalls are principally troubling for two reasons:

1. Their volume is a nuisance both to recipients and carriers because even when unanswered, they unnecessarily consume time and network resources.
2. They contain misleading or illegal content to defraud consumers.

The first troubling issue itself can assist with the mitigation of the problem. The sheer volume of calls, particularly those with shared characteristics, enhances the ability to perform statistical analyses on them. However, it is important to differentiate between illegal and legal robocalls, both of which may display high call rates. So, focusing on call volume alone is not sufficient.

The second issue is more challenging to use as a basis for mitigation because it requires knowledge of the call content and the caller's intent. It is highly unlikely that humans could screen all incoming calls' content. An alternative is using artificial intelligence (AI) to determine the nature of the call prior to its delivery to the intended recipient. AI-powered screening is not economical and not readily scalable. It also may create further user trust issues and have privacy and other policy and legal concerns.

Absent such pre-screening, the only current way to assess a call's probable content is to:

- Take feedback on the content of calls that have been answered.
- Note the other characteristics of the answered calls based on the call metadata, etc.

This knowledge enables techniques that apply blocking or other appropriate treatments to calls with similar characteristics and/or give the called party information about the likelihood that the call is illicit.

The industry has chosen to use call screening techniques that rely on information other than the content of the call being screened. These techniques consider other types of information describing the call, such as the calling party ID and its veracity, the frequency of calls from a given originator, and other signaling details. By correlating call metadata and calling statistics with recipient complaints, it is possible to judge which calls are likely illicit and which are not, and then take appropriate action. This report provides insights into the existing network architecture and services prior to the current major outbreak of robocall-based scams, the characteristics of illegal robocalls, the gaps, and challenges identified when considering different solutions, as well as the fact that no single technique can be 100% successful on its own.

To help readers comprehend how these various mitigation techniques are woven together, Section 13 describes a structure and methodology for classifying the component techniques described in the subsequent sections. It also outlines how they are commonly combined to provide comprehensive robocalling mitigation.

4

DEFINITIONS, ACRONYMS, AND ABBREVIATIONS

DEFINITIONS, ACRONYMS, AND ABBREVIATIONS

For a list of common communications terms and definitions, please visit the ATIS Telecom Glossary at https://glossary.atis.org.

4.1 DEFINITIONS

Note: The following definitions are only for this document.

Illegal Robocalls: Illegal robocalls are those made in violation of government laws and other regulations. Often these calls are used to conduct unsolicited lead generation or to perpetrate a scam. As used in this report, this term does not include individual calls that may be illegal on a single-incident basis, such as unintentional Telephone Consumer Protection Act (TCPA) violations. Common illegal call examples include mass-market unsolicited lead generation with no prior consent, impersonation attacks often using spoofing and extortion/manipulation campaigns such as the "tech support scam." Spoofing with malicious intent is a violation, according to the Truth in Caller ID Act of 2009.

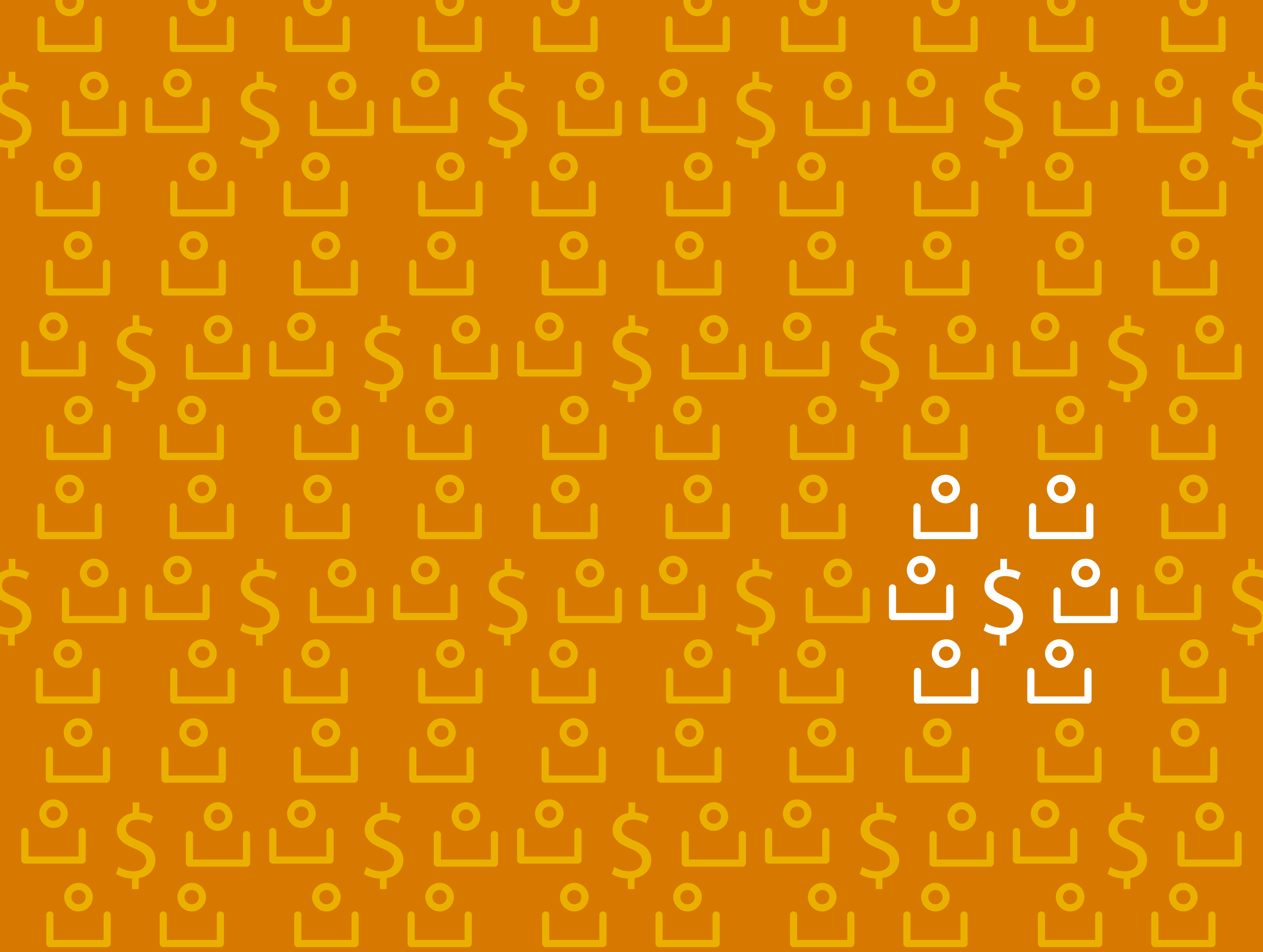
Types of illegal robocalls can be broken into the following categories:

1. **Pure Scam:** Blatantly illegal calls such those masquerading as the Internal Revenue Service (IRS), Social Security, and Apple support.
2. **Deceptive:** Calls claiming to sell a legal product, but you do not get what you pay for.
3. **Non-Compliant:** Legal products or services sold in violation of federal or state laws or regulations (e.g., TCPA violation).

Nuisance robocalls: Calls that are not illegal but are perceived as unwanted by consumers. Common nuisance calls include telemarketing solicitations, surveys, political solicitations, and some debt collection activities.

4.2 ACRONYMS AND ABBREVIATIONS

AI	Artificial Intelligence
ARCEP	Autorité de Régulation des Communications Électroniques et des Postes
ATIS	Alliance for Telecommunications Industry Solutions
ACMA	Australian Communications and Media Authority
ADO	Authoritative Databases' Owner
BPO	Business Process Organization
BNetzA	Bundesnetzagentur
CATA WG	Call Authentication Trust Anchor Working Group
CNARG	Calling Name Routing Guide
CRTC	Canadian Radio-television and Telecommunications Commission
CSTGA	Canadian Secure Token Governance Authority
C/CSPs	Carriers/Carriage Service Providers
CTND	Central Telephone Number Database
CA	Certificate Authority
CLI	Calling Line Identification
CNAM	Calling Name
eCNAM	Enhanced Calling Name
CSP	Communications Service Providers
CPE	Customer Provided Equipment
CPaaS	Communication Platform as a Service
CVT	Call Validation Treatment
DID	Distributed Identity
DLT	Distributed Ledger Technology
DNC	Do-Not-Call
DNO	Do-Not-Originate
CEPT	European Conference of Postal and Telecommunications Administrations
EV	Extended Validation
FCC	Federal Communications Commission
FTC	Federal Trade Commission
FMS	Fraud Management Systems
GSMA	Global System for Mobile Communications
HRPG	Hospital Robocall Protection Group
ISO	International Organization for Standardization
IETF	Internet Engineering Task Force
IP	Internet Protocol
IMS	IP Multimedia Services
KYC	Know Your Customer
NANC	North American Numbering Council
NIPCA	Non-IP Call Authentication
NANP	North American Numbering Plan
OCN	Operating Company Number
OEM	Original Equipment Manufacturer
OSP	Originating Service Provider
OOB	Out of Band
PTSC	Packet Technologies and System Committee
PII	Personal Identifiable Information
PSAP	Public Safety Answering Point
RCD	Rich Call Data
RCD-AS	RCD Authentication Service
RCD-VS	RCD Verification Service
RND	Reassigned Numbers Database
RAG	Risk & Assurance Group
SEISMIC	Stopping Exploitation of Internetwork Signaling by Mitigating Illegitimate Communications
STI	Security Telephone Identity
SIP	Session Initiation Protocol
SHAKEN	Signature-based Handling of Asserted information using ToKENs
SMS	Short Message Service
SP	Service Provider
SPC token	Service Provider Code token
STI-GA	Secure Telephone Identity- Governance Authority
STIR	Secure Telephony Identity Revisited
TCPA	Telephone Consumer Protection Act
TCCCPR	Telecom Commercial Communications Customer Preference Regulations
TKG	Telekommunikationsgesetz
TSR	Telemarketing Sales Rule
TRACED Act	Telephone Robocall Abuse Criminal Enforcement and Deterrence Act
TAS	Telephony Application Server
TRAI	Telecom Regulatory Authority of India
TDM	Time Division Multiplexing
TN LOA	Telephone Number Letter of Authorization
TN	Telephone Number
TNSP	Telephone Number Service Provider
TSP	Terminating Service Provider
UE	User Endpoint
UDP	User Datagram Protocol
UNI	User Network Interface



5

ROBOCALLING ECOSYSTEM STAKEHOLDERS

ROBOCALLING ECOSYSTEM STAKEHOLDERS

This section details the stakeholders involved in the robocalling ecosystem by describing their role, the ecosystem's requirements, the unintended consequences of robocall mitigation techniques, and current challenges to overcome.

5.1 SUBSCRIBER

5.1.1 Role

Subscribers are commonly an addressable individual using a single phone number who subscribes to this service from a telephony SP.

5.1.2 Inputs/Outputs

Subscribers use their phones to place calls out to the telephony network, expecting the SP to forward the call toward the destination. Subscribers also use their phones to be alerted of incoming phone calls and decided whether to answer them depending on their preference.

5.1.3 Needs

5.1.3.1 Restore Trust in the Communications Network by Mitigating Illegal Phone Calls

Subscribers need not be victimized. They do not have to be interrupted, threatened, coerced, or manipulated by an illegal caller industry. Subscribers need to know that when their phone rings, the call is from a legitimate person or enterprise calling with a valid need.

5.1.3.2 Know the Caller's Identity

A subscriber would benefit from having additional information regarding an incoming call. Examples include a less limited name (Calling Name (CNAM) is restricted to 15 characters) and a business/organization logo that helps identify the context of the call.

5.1.3.3 Assurance that the Caller is Legitimate

For incoming calls, subscribers should know that the caller's number and identity can be trusted and accurately reflect who is calling.

5.1.3.4 Assurance that Outbound Calls are Signed and Authorized

For outgoing calls, subscribers should be assured that their calls receive the same treatment of assurance that they can be trusted as not spoofed, thus making it more likely that their calls will be answered.

5.1.3.5 Consumer Education

Emerging call authentication technologies being deployed include Secure Telephony Identity Revisited (STIR)/ Secure Handling of Asserted information using toKENs (SHAKEN) and analytics services with capabilities to flag or allow calls to be blocked. Consumers need to be educated about how the results of these processes are presented to them and how to make the best use of that information for their protection.

5.1.4 Challenges

5.1.4.1 Limited Caller Name Data, Often at a Premium

At this time, some carriers show a separate charge for universal "Caller Name." Some of their customers subscribe to Caller Name, while others opt out, possibly due to it being a separate charge. Without caller name information, subscribers receive incoming calls with no information directly identifying the caller. This lack of caller name information makes it challenging for subscribers to differentiate between calls they want to answer and those they do not.

5.1.4.2 Caller ID (Number) Spoofing

Caller ID spoofing may lead to consumers falling victim to phone scams. Illegal robocallers may use spoofing to impersonate a known business, spoof to make a number feel more "familiar" (neighbor spoofing) or simply spoof to avoid detection.

Subscribers who are unfamiliar with the concept of spoofing may block a phone number in consequence of receiving a spoofed illegal call, not realizing they are blocking a legitimate caller number. Some consumers use blocking apps on their mobile devices. These solutions often rely on crowdsourcing: the popular agreement of many users to determine if a number is currently bad. This can have an adverse effect on legitimate callers by preventing emergency alerts from reaching people if those numbers were spoofed and flagged as suspect by crowdsourcing.

Typically, if their call is unanswered, scammers will leave a voicemail message with a way to contact them, all while continuing to impersonate a legitimate business such as a bank. They may leave a different callback number or even a website with a domain name similar to the business they are impersonating. These are examples of how a spoofed calling number opens other avenues for consumers to become victims beyond the call itself.

5.1.4.3 Errors in Call Flagging

Flagging refers to the practice of marking calls as potential nuisance or fraud based on the verdict of an analytics service. The call label applied to flagged calls uses the CNAM channel. In some instances, an application, which the SP itself may provide, on the device can source the label from an external system providing analytics services. In both cases, any CNAM label provided by the enterprise is overridden.

False positives (e.g., where a legitimate call is incorrectly labeled as “scam likely”) can lead to consumers not picking up calls that they actually want. Consumers may not be notified if the call flagging error is discovered and corrected. Instead, they rely on a mixture of the caller ID in their call logs or voicemail to decide if they should take action on a call. Their lack of awareness of a correction could affect their decision to act on a given call.

Analytics services need to ensure that they provide consumers with accurate and consistent call labeling. Doing so frees consumers from the task of correcting these inaccuracies themselves.

5.1.4.4 Transparency in Call Blocking

Call blocking refers to the practice of blocking calls based on the verdict of an analytics service or at the subscriber’s request. Most services let users control which types of calls to block. Many services simply block calls identified as fraud but provide subscribers with the opportunity to opt out.

Subscribers may not be informed when their SP blocks a call without the use of a companion application on their phone. Subscribers may not fully understand their call blocking choices or how to adjust them.

5.1.4.5 Outgoing Calls Not Being Answered

When people call others whom they have never called before, their calls may go unanswered due to the recipient not recognizing the number. This lack of number recognition erodes the usefulness of using voice calls as a communication channel for subscribers and may result from the lack of trust in the communications network.

5.1.4.6 Ability to Revoke Prior Consent

The TCPA says that “a called party may revoke consent at any time and through any reasonable means. A caller may not limit how revocation may occur.” With no clearly defined mechanism in place, the ability to opt out of prior consent remains challenging for subscribers.

5.2 ENTERPRISE

5.2.1 Role

Legitimate enterprises often employ call/contact centers where employees specialize in customer communications and act as the business’s front line towards subscribers. These call centers both originate and terminate calls from subscribers and often have a need for multi-sourcing and multi-homing of phone numbers for cost and redundancy purposes.

5.2.2 Inputs/Outputs

5.2.2.1 Inputs

Enterprises typically consider their numbers to be high-value assets because they are well known to their customers. Take the example of a company that provides enterprises with incident management services, including real-time monitoring and notifications. These communications are time-sensitive, critical, and lawful. This company places great value on its outbound number because its customers recognize it and often have it saved to their contacts to ensure they receive the call.

5.2.2.2 Outputs

Enterprises make phone calls to their customers either directly or through a Business Process Organization (BPO). A BPO may act and communicate on behalf of an enterprise and require an enterprise’s phone numbers to identify itself as the enterprise towards customers. Additionally, many enterprises use multiple outbound communication SPs, requiring this same caller ID originating with multiple Originating SPs (OSPs).

5.2.3 Needs

5.2.3.1 Accuracy in Call Treatment

Enterprises need analytics services to accurately identify their calls and not mis-flag or block legitimate callers as fraudulent.

5.2.3.2 Transparency in Call Treatment

Enterprises need visibility into whether any of their calls are blocked or labeled by analytics services at Terminating SPs (TSPs), and visibility into any specific labeling. They also need to understand under the TSP's criteria for any labeling or blocking. Blanket calling party notification must be avoided because it could provide valuable intelligence about how to avoid detection.

5.2.3.3 A Direct and Simple Dispute Process Against Analytics Services

Enterprises need a way to challenge labeling and/or blocking of outbound calls within a reasonable time frame. This process should not unduly burden them with trying to find the right organizations to contact or having to pass through multiple channels.

5.2.3.4 Standardized Method to Register their Validity

Because of the proliferation of illegal robocalls, legitimate enterprises need to be able to validate their identity and their association with various numbering resources. They need a simplified flow for registering important information about themselves and their call activity and for knowing that analytics services will use their information.

5.2.3.5 Ability to Associate Business Identification with Calls

Enterprises need a method for providing identifying information about themselves and knowing that this information will be represented to their call recipients. Ideally, this information can include the intent of the phone call ("campaign reason").

5.2.3.6 Guaranteed Display of Business Identification

Businesses go to great lengths to identify themselves and verify their legitimacy. As a result, they expect their CNAM, for example, to be displayed to all recipients of their calls.

5.2.3.7 Support for Robust Call Information

Enterprises would like to have their identity properly displayed, including more information such as logos and their full business name or organization. This additional information should be displayable on any modern device.

In addition to having a clear identification of the enterprise to the receiving party, enterprises may also desire to add the reason for calls. Typical use cases include tying contextual information such as "Calling About Your Reservation" or "Appointment Reminder" that allows the subscriber to have even more granular information to decide whether to pick up the call.

5.2.3.8 Protection Against Impersonation Attacks

Enterprises are frequently the victim of impersonation attacks where scammers spoof their phone numbers to fool call recipients. This spoofing directly harms the enterprise's reputation. These calls need to be detected and flagged/blocked, and any caller ID information should not be shown so these calls do not receive any credibility.

5.2.3.9 Protection from Hijacking Attacks

Enterprises can have their toll-free numbers hijacked for illegal robocalling campaigns.

5.2.3.10 Protection from Unwanted Calls

Like consumers, enterprises are afflicted with inbound unwanted and illegal call traffic that wastes time and money.

5.2.4 Challenges

5.2.4.1 Legitimate Spoofing

Due to the use of BPOs and multi-sourcing arrangements, the need for legitimate use of spoofing is critical to many enterprises. Any solution designed to detect call spoofing will have the challenge of correctly treating these legitimate spoof scenarios.

5.2.4.2 Enterprises Rotating Through Phone Numbers

Partly because of mis-flagging by analytics services, enterprises are increasingly rotating through active phone numbers. This rotation creates challenges in maintaining a registry of legitimate call activity. It also removes any meaningful history of activity under a single phone number, limiting the opportunity for analytics services to correct any possible errors and avoid future errors. In many cases, rotating through numbers increases the enterprise's customers' suspicion. They will use internet search engines to try to determine if the calling number legitimately belongs to the enterprise. Suppose a new number is being used where the customer is unable to attribute it to that enterprise. In that case, the customer will typically and swiftly flag that number as spam or a scam, quickly increasing damage to the reputation of that number.

5.2.4.3 Poor Detection of Impersonation Spoofing

Today, there is no guarantee of a signal being available to analytics services that a call has been spoofed. The lack of such signal prevents analytics services from isolating the malicious behavior of the spoofed calls from the business' legitimate behavior. Analytics services are often forced to take an "all or none" decision with these calls, either increasing false positives or reducing consumer protection. Outbound call-answer rates fell 30% in 2019 because so many legitimate calls were mistakenly blocked.[9]

5.2.4.4 Private Network Caller Hygiene

There are industry standards and practices that create consistency among SPs for passing calling party information associated with voice calls. However, private network operators (e.g., enterprises) have not been educated or held to the same standards and practices. Thus, many private network operators may not be aware of the significance of calling party information hygiene and may outpulse calling party information that is considered invalid by SP networks (e.g., non-E.164 formatted numbers). As a result, the outpulsing of alpha characters or numeric digits that do not conform to the E.164 format will be less likely to be answered and more likely to be blocked.

5.3 PUBLIC ACTOR

5.3.1 Role

Schools, non-emergency services, local and regional government bodies, and other similar actors use the telephony network to make calls and send texts to inform or alert citizens. As a timely public health example in the time of COVID-19, contact tracers struggle with getting people to answer calls.[10]

5.3.2 Inputs/Outputs

See Enterprise Section as it is largely shared.

5.3.3 Needs

See Enterprise Section as it is largely shared.

5.3.4 Challenges

See Enterprise Section as it is largely shared.

5.3.4.1 Lack of Prioritization for Calls

The calls made by these public entities are unable to get prioritized treatment.

5.3.4.2 Risk of False Positives

The traffic profile of calls from a public actor may appear as an increased volume of calls using a dormant calling number the previous hour or day. This call pattern historically runs the risk of being mislabeled.

[9] Connections Magazine, "Caught in the Crossfire: Contact Rates Continue to Decline," April 30, 2019, https://www.connectionsmagazine.com/article/outbound-call-centers-on-rcp/.

[10] KOMU News, "Contact Tracers Struggle with Getting People to Answer Calls," October 6, 2020, https://www.komu.com/news/contact-tracers-struggle-with-getting-people-to-answer-calls/article_a5b4afd8-c958-5bda-aaaf-18dd9be59612.html.

5.4 COMMUNICATION PLATFORM AS A SERVICE (CPAAS)/TELEPHONE NUMBER (TN) RESELLER

5.4.1 Role

Communication Platform as a Service (CPaaS)/telephone number (TN) Resellers are actors that, while not being OSPs themselves, allow enterprises to acquire TNs and originate and terminate calls from and to the enterprise platform. Originated calls are forwarded to an OSP on behalf of the enterprise. A CPaaS serves an important role in enabling programmatic access using APIs to the telephony network. These APIs enable enterprises and other organizations to create applications that integrate with the public telephony network without requiring telecom expertise and without a direct connection to the telephony network.

5.4.2 Inputs/Outputs

A CPaaS typically integrates with its customers using APIs that control resources such as phone numbers, calls, and text messages. The CPaaS then translates those APIs calls to a telecom level integration with OSPs and TSPs that relay calls and text messages onto the public telephone and texting networks.

5.4.3 Needs

5.4.3.1 Ability to Act as a Trusted Entity in the Telephony Network

A CPaaS acts as a broker of access to the telephony network and would preferably represent itself and its customers as trusted entities in the telephony network. The CPaaS owns the customer relation to the end customer rather than the OSP/TSP.

5.4.4 Challenges

5.4.4.1 Inability to Act as a Trusted Entity in the Telephony Network

A CPaaS has to rely on an OSP to initiate authenticated calls to the network because there currently is no mechanism for the CPaaS to represent itself or its customers as trusted entities that can digitally sign calls.

5.5 ORIGINATING SERVICE PROVIDER

5.5.1 Role

The OSP acts as the first carrier entity that provides access to the network. It has a customer relation with consumers/businesses/organizations that want to originate calls on the network.

Note that in the call authentication ecosystem, the role of OSP, and likewise TSP as described below, may be fulfilled by a traditional SP or another entity such as an interconnected VoIP provider or other reseller of telephony services. The definitions of OSP/TSP as they relate to call authentication responsibilities are subject to laws, regulations, and industry policy.

5.5.2 Needs

5.5.2.1 Reliable Delivery of Authenticated Calls

To serve its customers, the OSP must ensure that its calls get properly delivered to the intended destination with call authentication intact.

5.5.3 Challenges

5.5.3.1 Call Authentication Not Delivered with the Call

Even though the OSP delivers calls with call authentication, for various reasons it has the potential to be lost in transit to the TSP, even though the TSP can verify a STIR/SHAKEN PASSporT.

5.5.3.2 Identify Enterprises Originating Traffic

Not only do legitimate enterprises face the need to validate their identity, voice SPs also need to identify their enterprise customers. Customer due diligence applies to inquiries made about the customers to decide whether business should be undertaken or continued with the customer. A landmark FTC decision[11] further drives the expectation for customer due diligence by the SP to prevent voice SPs from conducting business with fraudulent entities. In addition to proper

[11] Federal Trade Commission, et. al. v. Educare Centre Services, Inc., et. al., U.S. District Court for Western District of Texas, Case No. 3:19-CV-196.

identification of an entity, the industry, type of calls, compliance, and association with known bad actors forms the Know Your Customer (KYC) framework for voice SPs.

Due to the fragmented approach of KYC practices, Congress expressed its support for a robust call authentication system to include the identification of a calling party.[12] Specifically, as part of the Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act, Congress directed the Commission to "issue best practices that providers of voice service may use as part of the implementation of effective call authentication frameworks… to take steps to ensure the calling party is accurately identified."[13] On February 27, 2020, the FCC directed the North American Numbering Council (NANC), via its Call Authentication Trust Anchor Working (CATA) Group, to recommend best practices satisfying Congress's directive if adopted by the Commission. On September 24, 2020, the CATA working group published best practices,[14] including but not limited to the vetting process either directly or through a third-party vetting provider.

5.6 TERMINATING SERVICE PROVIDER

5.6.1 Role

The TSP hosts a phone number on behalf of a subscriber or an enterprise, terminates the call, and provides the "last mile" connection to the destination subscriber. In many cases, the TSP provides the analytics service of blocking and/or labeling calls that terminate to the subscriber. The analytics service function may be outsourced to a third party.

5.6.2 Inputs/Outputs

The TSP receives calls for termination from interconnected SPs, either directly from the originating provider or through a transit provider. Pursuant to the STIR/SHAKEN roll-out, TSPs may receive calls with call authentication information, have the ability to verify the OSP's assertions about arriving calls, and may forward this information to the destination subscriber, allowing for a per-call determination on whether the caller ID is authenticated.

5.6.3 Needs

5.6.3.1 Trust in the Communications Network

TSPs rely on subscriber line and per-call charges that depend on the public telephony network's overall utility for the subscribers and call originators. As a result, the TSP's business is threatened by distrust in telephony due to robocalling and telephony for illegal and nuisance purposes.

5.6.3.2 Ubiquitous Call Authentication

If all calls arrive with STIR/SHAKEN PASSporTs, illegal call spoofing may be reduced as a fraud vector, which would likely lead to higher trust in telephony as a communication medium.

5.6.3.3 Guidelines for Blocking and Labeling

Although the TRACED Act gives TSPs safe harbor for some blocking, it does not provide guidelines, or industry best practices, for when to block or label an incoming call. The FCC has provided a non-exhaustive list of exemplary call blocking programs.[15]

5.6.4 Challenges

5.6.4.1 Non-authenticated Calls

As long as a significant portion of arriving calls are not authenticated, the use of call authentication as a trust signal to the subscriber will be limited.

5.6.4.2 Unclear Guidelines for Blocking and Labeling

In lieu of regulation, TSPs, OSPs, analytics services, and industry organizations may wish to work toward developing recommendations and best practices that provide guidance yet allow for flexibility and maintaining fair competition. See Section 19 for recommendations.

[12] Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, S. 151, 116th Congress, 2019, at § 4(b)(l).

[13] Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, S. 151, 116th Congress, 2019, at § 4(b)(7).

[14] NANC Call Authentication Trust Anchor Working Group, Best Practices for the Implementation of Call Authentication Frameworks, September 24, 2020, https://docs.fcc.gov/public/attachments/DOC-367133A1.pdf.

[15] Advanced Methods to Target & Eliminate Unlawful Robocalls and Call Authentication Trust Anchor, FCC No. 19-51, CG Docket No. 17-59, WC Docket No. 17-97, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, (released June 7, 2019), para. 35.

5.7 ANALYTICS SERVICES

5.7.1 Role

Analytics services are companies that provide a call analytics platform/service that a TSP may use to provide call labeling/blocking to mitigate unwanted and/or illegal robocalling.

5.7.2 Inputs/Outputs

5.7.2.1 Inputs

Analytics services use inputs from a large variety of sources to develop their reputation ratings. Primarily they collect historical call traffic patterns for all phone numbers. Many analytics services also receive consumer spam reports or complaints directly, as well as ingest those sent to the FCC and FTC. Analytics services will often use industry registry information including number validity/allocation status, business registry databases, etc.

The other primary input to analytics services is a single call, where they need to decide how to flag or treat that call. This input often will include call details such as the parties involved and Session Initiation Protocol (SIP) header signals where possible.

5.7.2.2 Outputs

The exact outputs vary by analytics service, but in general, they will determine if a call should provide a rating or be flagged as "unwanted" or "fraud." Many analytics services attempt to give more granular call classification information, such as category, some of which overlap with industry call purpose (e.g., debt collection, surveys).

The information provided by analytics services will often lead to a decision whether to block a particular phone call, although the analytics service may not make that decision directly. SPs or user preferences generally control which calls will be blocked versus allowed to continue.

5.7.3 Needs

5.7.3.1 Clear Indication of Call Spoofing Behavior

Analytics services are often left to decide based on phone numbers without knowing whether that number is actually making the phone call, potentially leading to errors in individual call treatment. Additionally, the called party response to the spoofed calls (e.g., call duration, spam reports) will be attributed to the phone number even if the call in question was legally or illegally spoofed. Analytics services need to differentiate between illegally spoofed and legally spoofed and non-spoofed calls, so their behavior and consumer responses can be treated separately.

5.7.3.2 A Source of Trusted Identity of Legitimate Enterprises

Enterprises may use similar calling patterns as traditional illegal robocalling entities, such as high volume, predominantly outbound, low answer rate, low call duration, and using an area code or six-digit neighbor number. These enterprises are the most difficult for analytics services to correctly classify, generally requiring the system to wait for user feedback to know who is using the number. Analytics services need a system whereby legitimate companies can register their identity and calling numbers, so analytics services can consider this claim of ownership when evaluating the call characteristics.

5.7.3.3 Identification Challenges for Emergency Public Safety Calls or Critical Calling NUMBERS

The highest risk for analytics services is an erroneous flagging of a critical service call, such as a Public Safety Answering Point (PSAP), police/fire station lines, medical service facilities, or other public safety notifications. Analytics services today make all efforts to prevent this possibility.

At this time, the FCC has not published a list of emergency public safety calls identifiers, also known as a critical calls list. Note that even a well-maintained database would be subject to abuse until illegal caller ID spoofing is eliminated. Bad actors would have an incentive to seek numbers on the list and spoof them, providing a virtual free pass to unlimited illegal robocalling because these numbers would, by being on a critical calls list, not be eligible for blocking.[16] Furthermore, implementing a unique signal in the call messaging indicating the call is "critical" would also open the door for bad actors to bypass analytics services.

The FCC requires voice SPs to make all reasonable efforts to ensure that calls from PSAPs and government outbound emergency numbers are not blocked. The FCC has repeatedly made clear that it expects all voice SPs to make all

[16] Advanced Methods to Target and Eliminate Unlawful Robocalls, FCC No. 20-96, CG Docket No. 17-59, Third Report and Order, Order on Reconsideration, and Fourth Further Notice of Proposed Rulemaking, (released July 27, 2020), para. 58.

reasonable efforts to ensure that critical calls complete and, in establishing the safe harbor, the TRACED Act directs them to do so.[17] [18]

To achieve these goals, the industry may still consider an organized source for critical call numbers.

5.7.3.4 More Robust Display Options for Caller Information

Especially for legal nuisance calls, the ideal solution is to properly label the purpose of the call (e.g., telemarketing, service reminder, customer support) while providing the caller's identity name so the called party can consider their relationship with that caller and decide if they want to pick up. In many circumstances, information is limited to a single string of 15 characters in length, even though modern original equipment manufacturer (OEM) equipment can display more. Analytics services may be able to give full context to the called party so they can make an informed decision. However, interfaces to the handset need to be updated to support more context.

5.7.4 Challenges

5.7.4.1 Inconsistency in Classification Structure

As stated previously, unwanted robocalls can be broken down into illegal call activity and legal nuisance calls. Legality is independent of TCPA compliance, which cannot be directly determined by an analytics service. Individual analytics services may not be able to distinguish between illegal and legal calls.

5.7.4.2 Lack of Control over Call Disposition

Most analytics services will state that they do not block calls. Analytics services only classify or rate phone calls. However, that classification may lead to the call being blocked in accordance with the preferences of the called party or the TSP. Inconsistency in the documentation and lack of industry agreement regarding call classification hinders progress in shaping an acceptable ecosystem for all stakeholders involved. Analytics services generally do not directly prevent calls from being blocked. They can only provide a classification that may lead to call blocking.

5.7.4.3 Need to Protect Service Behavior from Illegal Actors

Information that legitimate businesses would find helpful, such as their phone numbers' current analytics reputation status, also provides valuable information to illegal robocallers that want to maximize the success of their scams. By informing the calling party of its current reputation, the illicit party knows when it is time to switch to a new number to evade detection of their illegal calls once again. Communicating reputation creates a challenge for analytics services to support the legitimate call activity that may be wrongly flagged without empowering illegal callers to succeed more frequently.

5.7.4.4 Conflicting Tactics of Legal Nuisance Caller Industry

High-volume legal nuisance callers have adopted some of the tactics frequently seen in illegal robocaller traffic, including local number usage and accelerated turnover of calling numbers. These tactics make it more likely for numbers to be misclassified as an illegal caller based on the calling patterns.

5.7.4.5 Nuisance Caller Request for Anonymity

Analytics services want to provide accurate caller and call purpose information to the called party. However, this information may cause a decrease in call pickup rates for legal call traffic, especially if classified as a nuisance call. These callers do not want analytics services to classify the calls, even when that classification is accurate. This is often conflated by these callers with genuine misclassification errors, exaggerating the perception of a problem in analytic service accuracy.

[17] Ibid, para. 52.

[18] Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, S. 151, 116th Congress, 2019, at § 4(c)(2)(C).

6

ILLEGAL ROBOCALLER INDUSTRY

In 2018, illegal robocallers are estimated to have generated between 26.3 billion[19] and 47.8 billion calls[20] in the U. S. The exact number of independent companies operating at any one time is unknown, but a single company or conglomerate can generate a significant amount of traffic. Over the past few years, we have observed the take-down of top-volume generators, which can give some insights into this distribution:

- On Oct. 1, 2015, Aaron Michael Jones spoke to the FTC in Washington, DC. Around the same time, the FTC interviewed dozens of people connected to Jones' robocall enterprise. Interestingly, during the same period of August 2015 through February 2016, there was a 3x decrease in spam reports. This case demonstrates the growing sophistication within the industry. In total, almost 50 different companies under nearly 40 different names were connected to this case. Many of these companies were short-lived (<1 year) before they were replaced with another company. This was done both to remove fault from individuals and help obscure the purpose of these companies from federal agencies.[21] In May 2016, a default judgement was filed by the FTC in California's Central District Court against Jones and nine corporations linked to him. This judgement fined Jones 2.7 million dollars and was ratified in April 2017.
- In June 2016, Adrian Abramovich's shell company "Marketing Strategy Leaders" generated 96 million robocalls[22] in three months, accounting for 3.8% of the estimated illegal call volume[23] that year.
- In October 2016, the shutdown of an IRS Scam call campaign[24] centered out of India removed 95.3% of all consumer complaints of the IRS Scam and 27.1% of complaints in general to Hiya over a 30-day period.
- In March 2019, the FTC shut down four independent robocaller operations[25] attributed to billions of robocalls over an unspecified period of time. This led to no appreciable impact in overall unwanted call traffic or consumer complaints.
- In June 2020, the FCC proposed a record $225 million fine for a massive robocall campaign that made approximately 1 billion spoofed robocalls selling health insurance.[26]

All indications are that the illegal call industry has been growing more diverse over the past few years from a few major players that can potentially be responsible for 25% of all calls.

This boldness of the illegal call industry directly stems not just from the profitability of social engineering techniques and blanket marketing campaigns, but also from the difficulty that law enforcement faces when pursuing the originators. Tracing back the originating provider of illegal call activity is a complex, multi-step process to request information about that call from each network hop of its connection. Only recently, with the Industry Traceback Group's[27] efforts, has it become practical to do this in a reasonable amount of time, but the growing diversity in illegal callers means that the individual gains from pursuing a single caller are diminishing.

6.1 ILLEGAL CALL CAMPAIGN TYPES

The majority of illegal call campaigns fall within one of two types: fraud campaigns and lead-generation businesses.

6.1.1 Fraud Campaigns

These campaigns operate to solicit information or money or both out of call recipients, with no legitimate product or service offered. Fraud campaigns include scams and extortion related to the IRS, tech support and more.

[19] Ferris, Mike, "Scammers Capitalizing on COVID-19: Hiya Sees Over 850% Surge in Stimulus Check Phone Scams," https://hiya.com/robocall-radar.

[20] YouMail, "Nearly 48 Billion Robocalls Made in 2018, According to YouMail Robocall Index," January 23, 2019, https://www.prnewswire.com/news-releases/nearly-48-billion-robocalls-made-in-2018-according-to-youmail-robocall-index-300782638.html.

[21] Federal Trade Commission v. Aaron Michael Jones, et. al., U.S. District Court Central District of California, Case No. 8:17-CV-00058, https://www.ftc.gov/system/files/documents/cases/allorey_-_motion_for_default_judgment_-_with_attachments_4-10-17.pdf.

[22] Murdock, Jason, "Who is Who Is Adrian Abramovich? Miami Man Accused of Making 97 Million Robocalls Fights $120 Million Fine," Newsweek, April 19, 2018, https://www.newsweek.com/who-adrian-abramovich-miami-man-accused-making-97-million-robocalls-fights-120-892275.

[23] Hiya, Robocall Radar: 2018 Report, 2018, https://assets.hiya.com/public/pdf/RobocallRadar.pdf.

[24] Khan, Omar; Riley, Charles, "India Busts Bogus Call Centers for Posing as the IRS," CNN Money, October 6, 2016, https://money.cnn.com/2016/10/06/news/india-irs-scam-arrests/index.html.

[25] Khan, Omar; Riley, Charles, "India Busts Bogus Call Centers for Posing as the IRS," CNN Money, October 6, 2016, https://money.cnn.com/2016/10/06/news/india-irs-scam-arrests/index.html.

[26] Federal Communications Commission, "FCC Proposes Record $225 Million Fine for 1 Billion Spoofed Robocalls," June 10, 2020, https://www.fcc.gov/document/fcc-proposes-record-225-million-fine-1-billion-spoofed-robocalls-0.

[27] All referenced industry organizations in this Report are listed in Section 20.

One misconception of fraudulent campaigns is that they may be intentionally malicious or disorganized. In reality, neither is entirely true. A scam is often executed under contract by a call center, frequently overseas,[28] that is operating the scam as just another scripted contract for a customer.

6.1.2 Lead-Generation Campaigns

These common campaigns are illegal methods to generate new customer opportunities (or "leads") for legal businesses. These systems (such as the one used by scammers Aaron Michael Jones and Adrian Abramovich[29]) are structured specifically to lend legal plausibility to all players by using multiple layers of obfuscation (Figure 6.1).

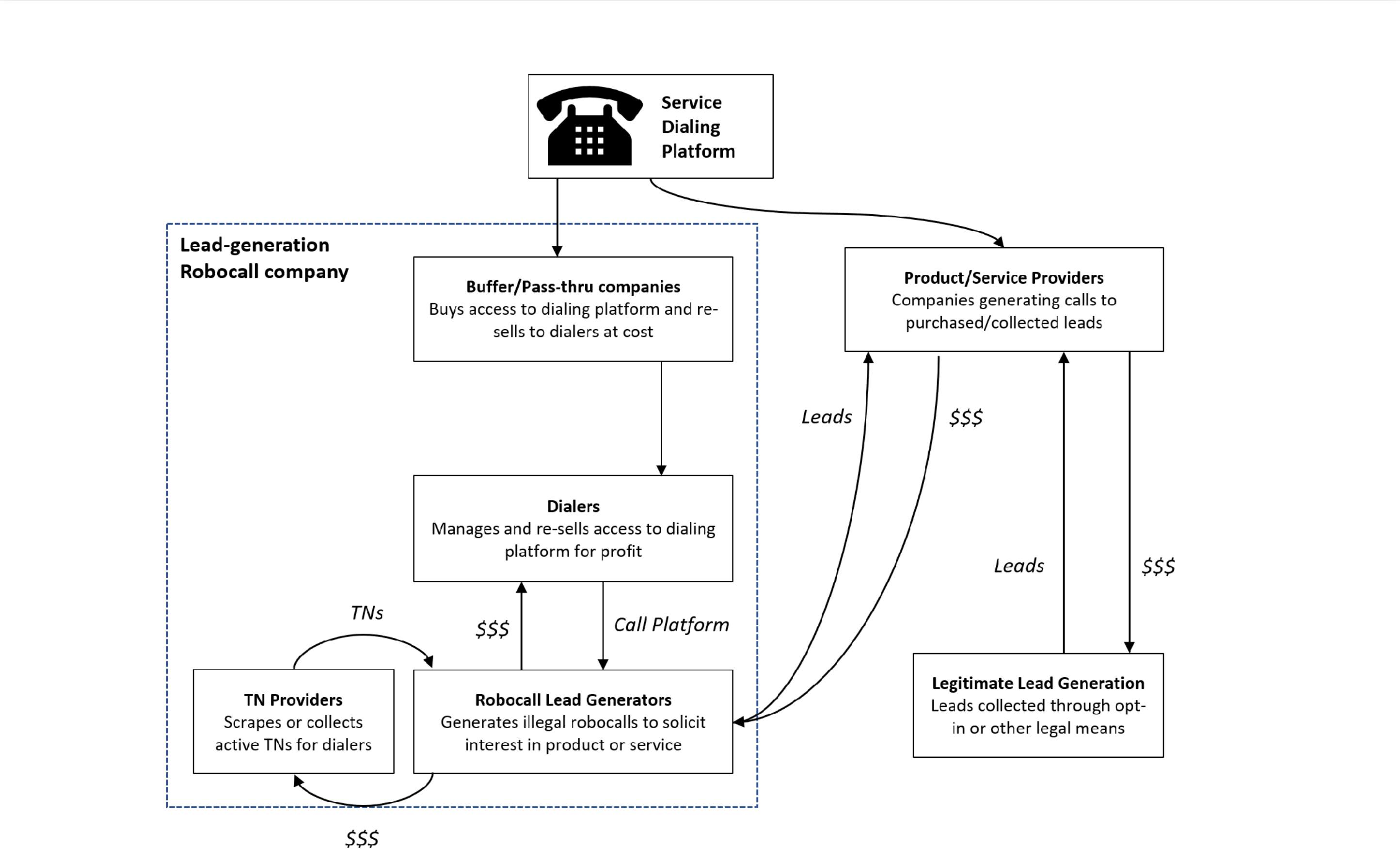

Service Dialing Platform
Lead-generation Robocall company
Buffer/Pass-thru companies
Buys access to dialing platform and re-sells to dialers at cost
Dialers
Manages and re-sells access to dialing platform for profit
TN Providers
Scrapes or collects active TNs for dialers
Robocall Lead Generators
Generates illegal robocalls to solicit interest in product or service
TNs
$$$
Call Platform
$$$
Product/Service Providers
Companies generating calls to purchased/collected leads
Leads
$$$
Leads
$$$
Legitimate Lead Generation
Leads collected through opt-in or other legal means

Figure 6.1: A Diagram of a Typical Lead-Generation Call System

Within this system, a shell company or companies stands between the organization and the dialing platform to protect that platform from direct legal assault through plausible deniability. That company passes through to any number of dialing agencies to purchase potential lead numbers from data providers and push illegal call traffic either directly, or through caller identification management services to modify caller ID for increased legitimacy. These call generators are able to generate the calls through a veil of legitimacy and redirect the resulting leads to operating businesses in exchange for compensation.

During a campaign, the caller network will offer a service and ask the victim to press a button if interested. When the victim presses 1, the call is transferred to a sales representative who then tries to close the sale. These campaigns may be illegal because they are unsolicited and/or if they falsely claim to represent legitimate businesses.

6.2 TECHNOLOGIES LEVERAGED IN CAMPAIGNS

Any illegal call behavior analysis needs to be separated into two key details: the method and the message. Frequently, the industry is using the term "robocaller" to reference illegal call activity specifically. However, robocalling is just one of several call generation methods at play, all of which can be either legal or illegal. Further, not all illegal calls are robocalls.

[28] For example, the podcast series "Reply AI,I" episodes #102 & #103, provide details about the India call center scam.

[29] Consumer Reports, "A Rogues' Gallery of Robocallers," April 2, 2019, https://www.consumerreports.org/robocalls/rogues-gallery-of-robocallers/

6.2.1 Robocalling

In general, "robocall" refers to any call where the audio is one or more pre-recorded messages without a live human on the line. The simplest robocalls will have a single promotional message, usually ending with a call to action, such as pressing a key to learn more. At that point, the recipient may be connected to a live human. This technique is used to allow for a high volume of calls with minimal support staff. The FTC governs robocalling under the Telemarketing Sales Rule (TSR).[30] One variation of robocalling is known as "avatar calling," leveraging soundboard technology, where a human listens to the call but presses buttons to deliver prerecorded responses to the call recipient. Avatar calling allows a single operator to field multiple calls simultaneously, reducing overall costs. Avatar calling was also deemed illegal in May 2017.[31] [32]

Examples of a legal message for robocalling include prescription reminders, schedule changes, or other voluntarily elected notification services.

The exact percentage of illegal call traffic that is technically robocalling is unknown, but it is known with certainty to not be 100%. This is especially true for the fraud campaigns, which may immediately attempt to engage with the victim rather than assess interest (as is typically done for the lead generation campaigns).

6.2.2 Autodialing

Nearly every campaign involves some amount of autodialing, where the call is initiated automatically as opposed to manually dialed by a human. The FCC and FTC govern the use of autodialers through restrictions included in the TCPA[33] and the TSR. These rule sets generally apply to the use of any equipment or software capable of generating or storing numbers and dialing them without human intervention, regardless of whether the numbers called are randomly or sequentially generated or come from calling lists. Additional state-level regulations may further restrict the use of autodialers.

Note that this is independent from robocalling. It is reasonable, and at times necessary, due to differences in the robocall law and the autodial law, for a human to manually initiate phone calls, then hand them off to an automated system for the actual call interaction (robocall).

6.2.3 Spoofing

"Spoofing" refers to the insertion of a TN into the 'From' header of a SIP INVITE phone call packet that does not match the actual phone number being used to generate that call. The FCC governs call spoofing under the Truth in Caller ID Act.[34] It generally applies to the use of call spoofing with the intent to defraud, cause harm, or wrongly obtain anything of value.

Examples of legal call spoofing are cases of witness protection, or legitimate business operations under multiple phone lines with a single primary business call destination line.

As with robocalling, it is unknown exactly what percentage of illegal call behavior uses spoofing, but it is known not to be 100%. It should be noted that not all illegal campaigns use spoofing.

6.3 TARGET NUMBER SOURCING

It is possible for an illegal call operation to set up an autodialer that calls phone numbers completely at random or randomly within the number block range in compliance with the North American Numbering Plan Administration (NANPA). However, as reported in 2010, only 47.9% of those numbers were assigned to subscribers.[35] Dialing unassigned numbers is a needless expense and exposes an illegal call company to easier detection by the SPs in possession of those numbers.

Additionally, it is far more efficient for illegal call companies to use a purchased, targeted number list.[36] These lists may be legal number lists leveraged in legitimate marketing efforts or illegally sourced, such as from data breaches. Scams and offers have a higher success rate when targeting appropriate victims. Examples include new homeowners for false home security systems, elderly for medical support, and recent immigrants claiming wrongly filed taxes.

The illegal call industry also generates these lists directly. It is believed that lists of active lines (determined by who answers a

[30] Federal Trade Commission, "Telemarketing Sales Rule, 16 CFR 310," https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/telemarketing-sales-rule.

[31] Greisman, Lois to Bills, Michael, "Letter Regarding September 11, 2009 Staff Opinion Letter on Soundboard Technology," Federal Trade Commission, November 10, 2016, https://www.ftc.gov/system/files/documents/advisory_opinions/letter-lois-greisman-associate-director-division-marketing-practices-michael-bills/161110staffopsoundboarding.pdf.

[32] Bob Traylor, "Avatar Calls Illegal After May 2017, Says FTC," November 17, 2016, http://www.donotcallprotection.com/blog/avatar-calls-illegal-in-6-months-says-ftc.

[33] Federal Communications Commission, "FCC Actions on Robocalls, Telemarketing," https://www.fcc.gov/general/telemarketing-and-robocalls.

[34] Federal Communications Commission, "Caller ID Spoofing," https://www.fcc.gov/consumers/guides/spoofing-and-caller-id.

[35] Federal Communications Commission, Telephone Numbering Data - June 30, 2010 Report, April 5, 2013, https://www.fcc.gov/general/telephone-numbering-data.

[36] e.g., https://www.salesgenie.com/.

call or calls that reach functioning voicemail systems) are sold within the industry. Additionally, the lead generation campaigns are essentially operating to generate target lists for resale, at times to legitimate businesses with no awareness of the illegal method by which they were sourced.

6.3.1. Robocall Detection Avoidance

Some robocall placement services are aware that their success rates are declining with the rise of over-the-top blocking solutions (typically offered directly to consumers as Android and iOS apps). Some are incurring additional expenses to curate their calling lists, such as performing carrier lookups prior to placing their robocall. Their perception is this will allow them to avoid calling a number that is not a possible lead or target and avoid detection by a robocall honeypot number.

6.4 ILLEGAL ROBOCALL INDUSTRY PROFITABILITY MARGINS

Illegal call campaigns are popular because they are profitable. Through the sale of business leads, farmed personally identifiable information (PII), and the income collected directly through extortion, callers are able to offset their operating costs. The primary operating costs for the illegal call industry are: Operator staff; Public Switched Telephone Network (PSTN) access; Dialing equipment rentals; and Fines (risk).

At least one report estimated the illegal call industry's overall operating costs at $438 million,[37] or approximately 5% of the revenue generated through scams and lead generation.

6.5 ONE-RING SCAMS

The TRACED Act requires the FCC to identify ways to tackle one-ring scams or "Wangiri" scams. Wangiri is a Japanese word for "one (ring) and cut." With one-ring scams, a scammer places a robocall to a number and hangs up after one or two rings in the hope that the recipient will call back. If the caller calls the number back, they are then connected to a number that results in charges to the caller, such as an international number, which is charged at a premium rate. This involves payment to deliver the call to its foreign destination generating intercarrier compensation payments that ultimately flow to, or are shared with, the original caller.

Detecting fraudulent calls is a considerable challenge due to the massive number of calls an operator handles per day. Fraud management solutions can assist in detecting one-ring calls by monitoring the high-risk numbers and discovering the calls made by scammers. Some operators have introduced blocking systems that detect the scammers and block the calls before they reach subscribers. Machine learning (ML) and AI can also be leveraged to detect fraud in early phases.

One recent solution introduced by the Risk & Assurance Group (RAG) provides a blockchain-based fraud management solution: the RAG Wangiri Blockchain Consortium.[38] The consortium includes some of the world's leading Communications SPs (CSPs) from North America, Europe, Africa, and Asia. Blockchain technology is used to create a decentralized and cryptographically secure distributed ledger of fraud-related information that can be used to share intelligence in near real-time about actual one-ring calls that have already occurred. To date, over 60 CSPs and seven Fraud Management Systems (FMS) globally have integrated into the RAG Wangiri Blockchain solution, with over 1 million numbers entered into the ledger.

Numbers entered into the database are "graded" on the likelihood of fraudulent activity based on the information entered by the consortium. However, some regulators will require 100% verification that the number is fraudulent before allowing the CSP to automatically block the number, which would require third-party test call generation or analytics services.

One issue with Wangiri fraud and databases is the timing. Most databases have old information. Fraudsters typically change numbers rapidly, and therefore a real-time detection solution would be needed. The databases are still needed due to fraudsters reverting to old numbers, or numbers being recycled.

Known methods to combat Wangiri fraud (one-ring scams) include:

- Utilizing valid number range databases (e.g., iconectiv's TruNumber Protect)[39]
- Shared numbers in a centralized database[40]
- Real-time detection based on machine predictive analysis tools and algorithms (e.g., GBSD Technologies' FINIS)[41]

[37] Robokiller, "Spam Calls 101: Important Facts Everyone with a Phone Should Know (Updated for 2020)," September 10, 2020, https://www.robokiller.com/blog/spam-calls/.

[38] Risk and Assurance Group, "RAG Wangiri Blockchain Consortium," https://riskandassurancegroup.org/rag-wangiri-blockchain-ledger/.

[39] iconectiv, "TruNumber Protect," https://iconectiv.com/trunumber/protect

[40] For a view of the RAG Wangiri ledger/map see: https://wangiriblockchain.riskandassurancegroup.org/Pages/LandingMap.aspx.

[41] GBSD Technologies, "FINIS: Fraud Interception & Network Integrated Signaling," http://gbsdtech.com/wpweb/fraud-blocking-overview/.

7

SHORT MESSAGE SERVICE (SMS) SPAM AND FRAUD

SHORT MESSAGE SERVICE (SMS) SPAM AND FRAUD

SMS spam and fraud have one common aspect with robocalling, as well as significant differences. As with robocalling, SMS spam and fraud messages are sent using E.164 addresses. Therefore, like robocalling but unlike email spam, the individual address of a target need not be known, and mass campaigns are possible without the perpetrators needing to obtain address lists. However, with SMS spam, it may be possible to analyze the contents of a message prior to delivery, enabling content-based mitigation techniques to be applied on a per-message basis. This brief section on SMS spam and fraud is therefore included in the report both for the sake of completeness, and to enable some comparisons to be made regarding possible mitigation treatments.

According to Mavenir and the Global System for Mobile Communications Association (GSMA), between 5% and 20% of all SMS messages are spam or fraud related.[42] SMS spam is often unsolicited advertisements delivered as text messages to mobile phones. It is annoying but harmless, such as advertising an unwanted product or service. However, a growing percentage of SMS spam falls into the category of scam or fraud. Typically, SMS fraud falls into one of three main categories, which are detailed below.

7.1 SPAM

SMS spam is where spoofed or illicit messages are sent to subscribers. In this case, the text looks like a legitimate message and encourages the recipient to hand over their personal data that unwittingly result in information disclosure or financial loss. "Smishing" is a social engineering technique combining spam, SMS originator spoofing, and social engineering techniques where the sender of a message pretends to be someone that the recipient knows, such as a bank or employer. With SMS read rates as high as 98%,[43] text messages are incredibly effective in reaching a global audience of all ages and walks of life, making it extremely lucrative for fraudsters.[44]

SPs use spam firewalls to analyze the message content and block messages determined to be illicit based on the spam rules. During COVID-19, there have been many types of messages that seem to have mitigated the SP spam filters.

7.2 INTERCONNECT FRAUD

Interconnect fraud occurs when the SMS is being terminated illegally on an SP network over SS7 interconnect, and the SP has no way to recover the cost from the interconnecting party. The mechanism used to identify and block this kind of fraud is an SMS firewall, where analytics services detect and prevent fraudulent terminating SMS messages from entering the network.

7.3 GREY ROUTES

Application-to-person (A2P) messaging is one of the most widely used communication methods for enterprise businesses. A grey route is A2P messaging that originates outside of authorized networks, specifically non-commercialized traffic where there is no agreement between the sender and the receiving network. Many grey routes use person-to-person (P2P) channels to support A2P messaging. The A2P messages are sent using long numbers to appear as P2P messages through other SPs and subscriber identification module (SIM) boxes to avoid paying for A2P charges. This traffic cheats operators out of expected termination fees, resulting in loss of revenue for the TSP.

7.4 CURRENT MITIGATION MEASURES

Current mitigation measures for SMS spam and fraud encompass a variety of proprietary methodologies and options such as frequency analysis, volumetric checks, pattern matching and offline analysis, and blocklisting. SMS fraud is becoming more sophisticated and is evading these traditional methods of detection. More advanced spam detection technology leverages AI and ML. ML detection algorithms adapt to the current network and subscriber's behavior and enable real-time detection. AI-powered SMS filters utilize deep learning AI systems to identify and filter spam SMS before they reach the recipient. These correlation techniques incorporate external learning feeds, including spam reporting services, centralized spam databases, URL reputation statistics, and call-back number reputation.

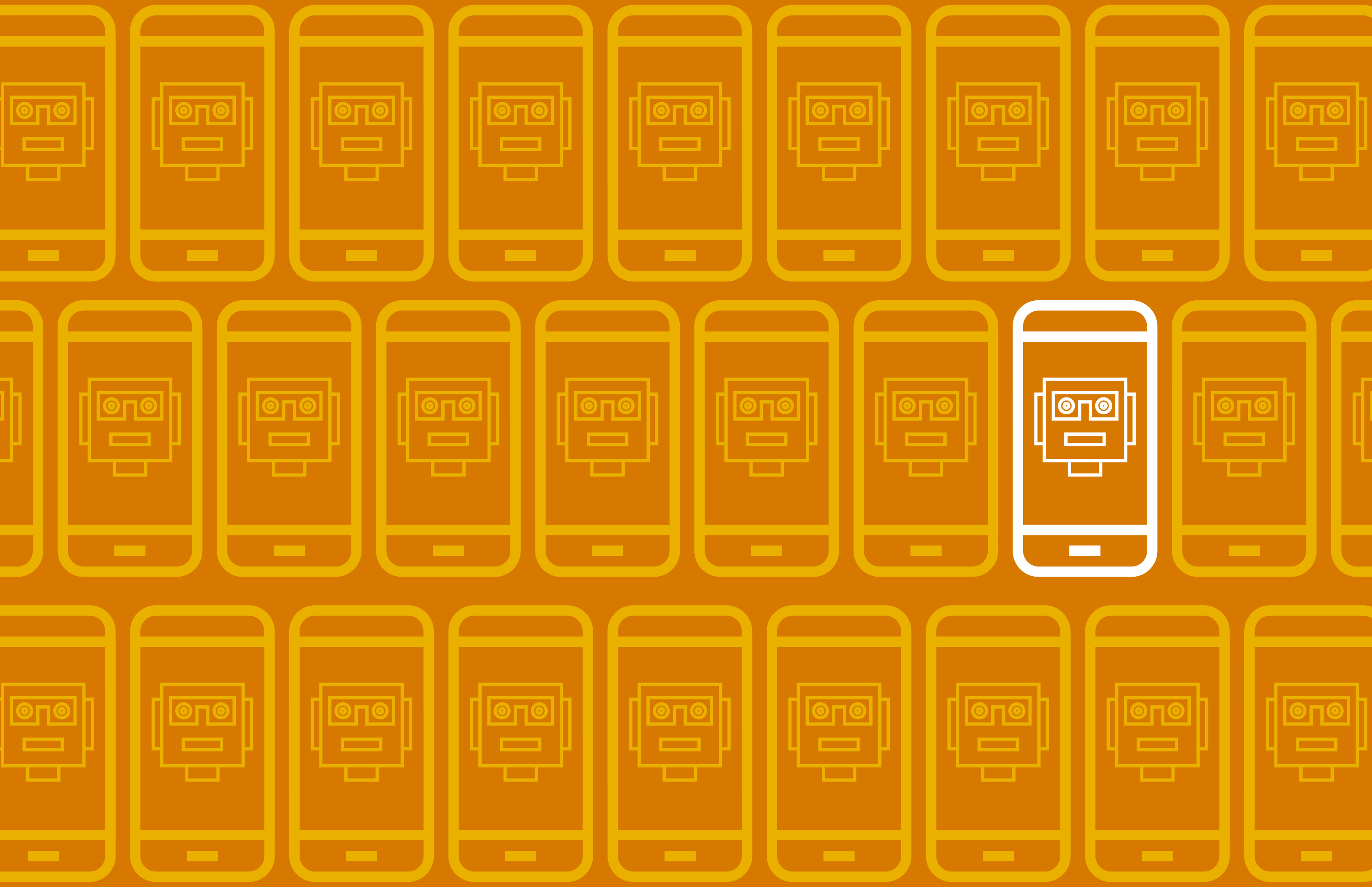
[42] Mavenir, "Spamshield/Messaging Fraud," https://mavenir.com/portfolio/advanced-services-applications/fraud-security/spamshield-messaging-fraud/.

[43] Dobrilova, Teodora, "35+ Must-Know SMS Marketing Statistics in 2020," TechJury, September 16, 2020, https://techjury.net/blog/sms-marketing-statistics/

[44] CEQUENS, "7 Deadly Types of SMS Fraud," July 9, 2019, https://www.cequens.com/story-hub/7-deadly-types-of-sms-fraud.

7.5 GAPS

Scammers are continually adjusting their delivery techniques to avoid detection. More effective spam and fraud control techniques are required for trusted enterprise A2P. Implementing a verified enterprise identity that could be authenticated together with a list of bad actor TNs that are shared across the industry would help provide better mitigation measures. Failure to secure the SMS platform in this way may drive enterprises to seek alternative trustable messaging services.The illegal call industry is constantly creating new scams and schemes to generate money, both to avoid detection and to increase their overall success rate. Scams are tested, successful ones will run rampant, and unsuccessful ones are retired.



8

ILLEGAL ROBOCALLERS AS AN ADVERSARY

8.1 NEIGHBOR SCAMS

One of the most blatant examples of this is the rise of the "neighbor scam." Between February 27 and May 6, 2017, the volume of unwanted calls using an impersonation of the first six digits of the called party's phone number ("neighbor spoof") more than quadrupled.[45] This technique remained more than 25% of all unwanted calls until December 2017. By that point, the popularity of this technique and the adoption of blocking solutions by analytics services led to a minor shift to only a five-digit match. That continued its popularity for another year before the callers shifted again.

In December 2018, the volume of illegal calls shifted to abandon the larger number match (which is easily recognizable) in favor of an area-code-only match on the callers, continuing to drive down the 5 and 6-digit match cases. Area-code match remains the most popular technique today.

This case study demonstrates how the illegal call industry is observant and reactive, just like any other profitable business. When this new technique was first widely adopted, it led to high pickup rates and became very popular. As both consumers and analytics services grew aware of this method, the illegal callers began their evolution to keep their success rate up.

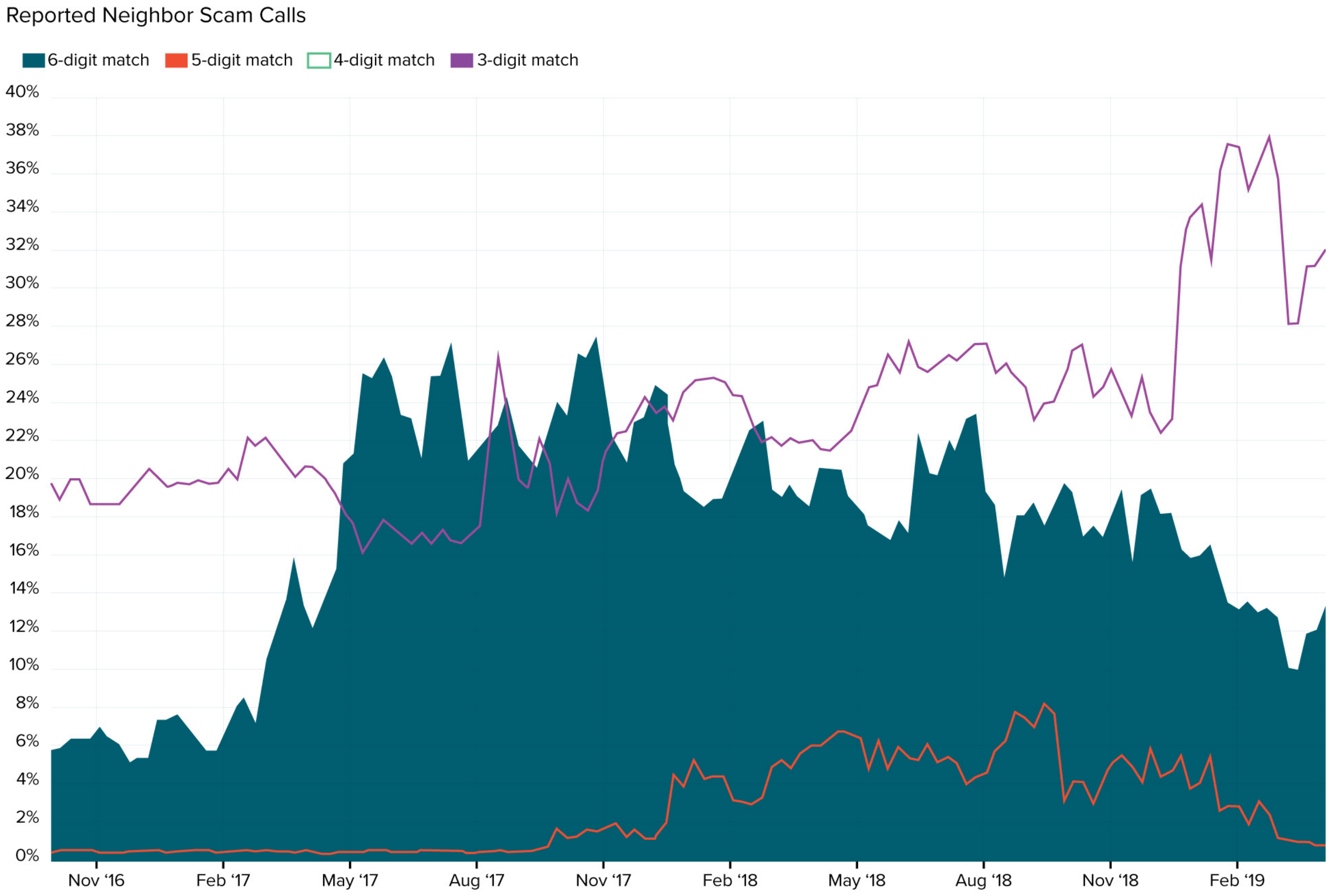


Figure 8.1: The Neighbor Spoofing Shifts to an Area-Code-Only Match

8.2 RESPONSES TO MAJOR EVENTS

Scammers often will target major world events, and explore new and unique campaign topics, all in an attempt to stay relevant and bypass a growing defense.

Most recently, criminals are attempting to exploit the COVID-19 pandemic worldwide through a variety of scams. The FCC has received reports of scam robocalls and hoax text message campaigns offering free home testing kits, promoting bogus cures, selling health insurance, and preying on virus-related fears.[46] Using caller ID spoofing, scammers pretend to be someone from

[45] Hiya consumer spam complaint trends.

[46] Federal Communications Commission, "Coronavirus Scams - Consumer Resources," December 11, 2020, https://www.fcc.gov/covid-scams

an official agency, such as the Social Security Administration, the Centers for Disease Control and Prevention (CDC), Medicare, or the World Health Organization (WHO).

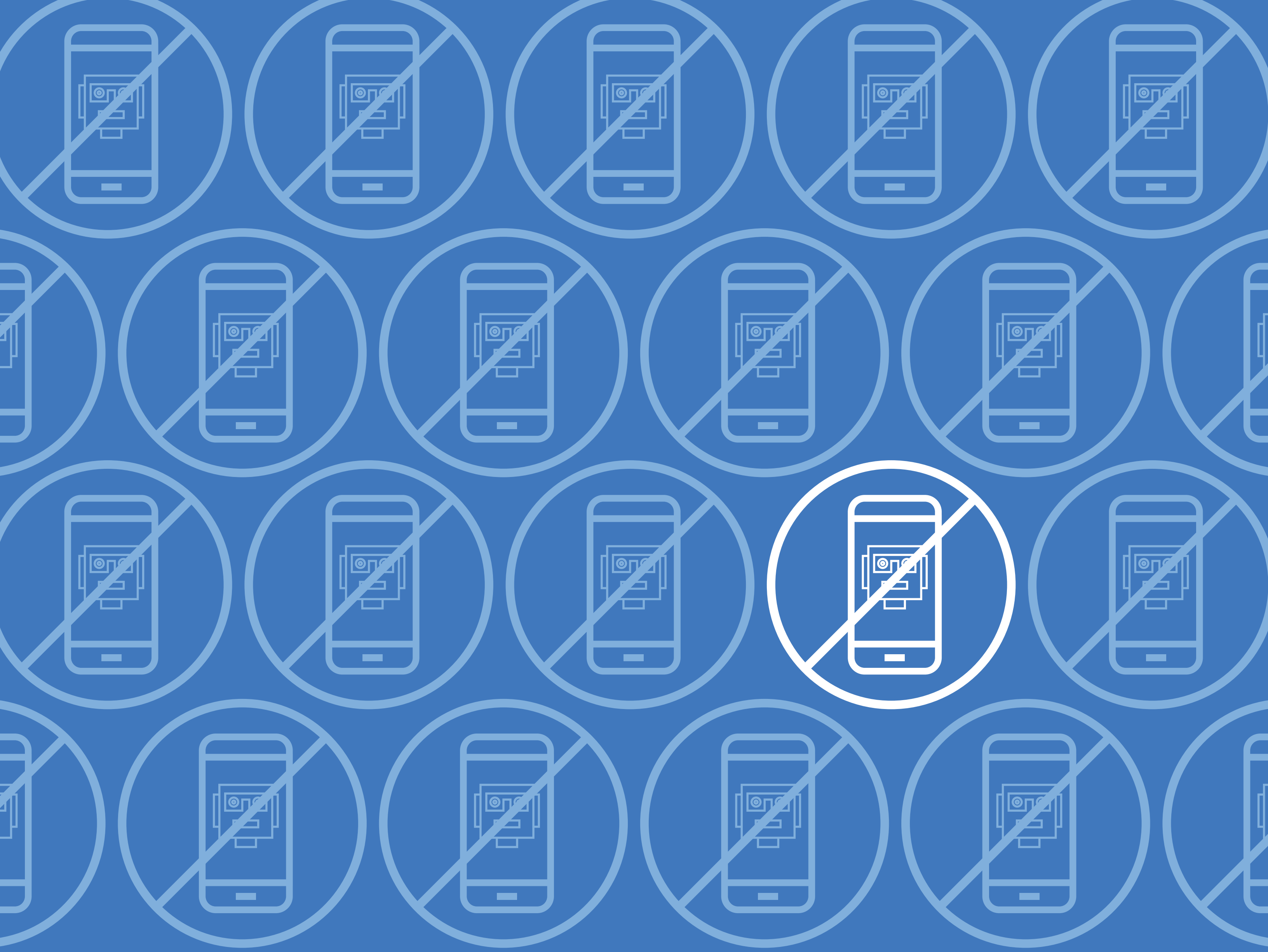
In response, the FCC and FTC have demanded that SPs do their part to stop coronavirus-related scam robocalls from bombarding American consumers. They specifically warned three gateway providers facilitating COVID-19-related scam robocalls originating overseas that they must cut off these calls or face serious consequences.[47]

From January to May 2020, the FTC and FCC sent joint letters to companies providing VoIP services warning them that routing and transmitting illegal coronavirus-related scam robocalls is itself illegal and may lead to federal law enforcement against them. A press release announcing action noted that these letters “alert the recipients that they have been identified as routing and transmitting coronavirus-related scam robocalls and tell them to stop such conduct immediately or face potential law enforcement actions.” The FTC and FCC identified the specific companies in question, noting that their refusal to work with the USTelecom Traceback Group is “particularly problematic.”[48] [49]

[47] Federal Communications Commission, “FCC, FTC Demand Gateway Providers Cut Off COVID-19 Robocall Scammers,” Media Release, April 3, 2020, https://docs.fcc.gov/public/attachments/DOC-363522A1.pdf.

[48] Federal Communications Commission, “FCC, FTC Demand Robocall-Enabling Service Providers Cut Off COVID-19-Related International Scammers,” Media Release, May 20, 2020, https://docs.fcc.gov/public/attachments/DOC-364482A1.pdf

[49] Federal Trade Commission, “FTC and FCC Send Joint Letters to Additional VoIP Providers Warning against ‘Routing and Transmitting’ Illegal Coronavirus-related Robocalls,” Media Release, May 20, 2020, https://www.ftc.gov/news-events/press-releases/2020/05/ftc-fcc-send-joint-letters-additional-voip-providers-warning?utm_source=govdelivery.



9

ILLEGAL ROBOCALLER IMPACTS

9.1 CALL VOLUMES

YouMail tracks mobile calls and voicemail received by owners of Android and iPhone devices and confirms that as of August 2020 in the U.S., 61% of all incoming calls are from a contact record saved on the device, while 39% are from callers who do not have a contact record on the device. The 39% of non-contact calls make up the majority of unanswered calls, which result in either a hang-up by the caller with no voicemail left or a voicemail message left for the device owner. Of these unanswered consumer calls that do not match a device contact in August 2020, over half can be correlated to a legal relationship between the call recipient and the calling party. Between 10% and 15% are positively identified as fraud or a likely TCPA violation by the caller.[50]

Figure 9.1 illustrates YouMail's estimates for monthly robocalls received in the US since 2015. The new plateau of 5 billion robocalls per month in October 2018 was up 200% from prior levels of roughly 2.5 billion per month established in 2017. Since October 2018, the volume of robocalls received in the US was steady, between 4 to 5 billion per month until April 2020. At this time, the effects of the COVID-19 pandemic radically disrupted call volumes across all industries. Although many pandemic-related robocalls began to emerge, the drop in telemarketing-oriented robocalls dropped the overall monthly average of all robocalls back to 2017 levels of 2.5 billion per month. At the time of this report, after six months of pandemic onset in the U.S., monthly robocall volumes have steadily climbed back to over 4 billion per month in October 2020.[51]

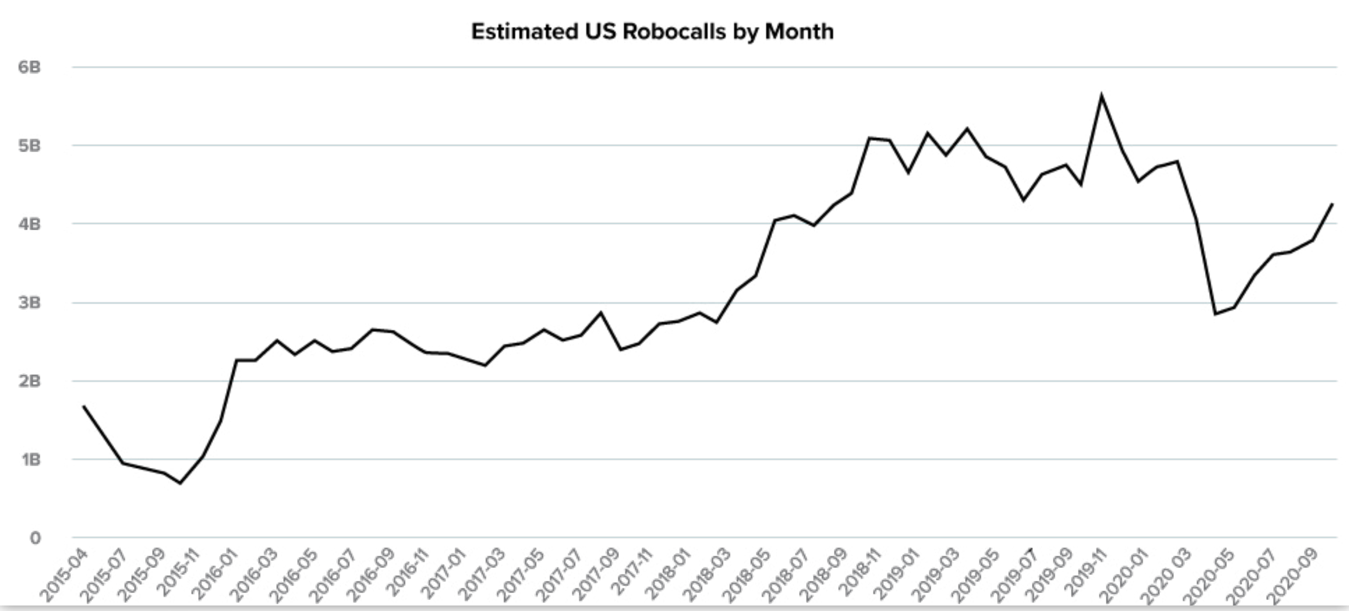


Figure 9.1: Robocalls Over Time

9.2 FCC CONSUMER COMPLAINT DATABASE

The FCC established the Consumer Complaint Center[52] for filing informal complaints for areas regulated by the FCC, including TV, phone, internet, radio, access for people with disabilities, and emergency communications. The largest category of complaints is related to robocalls. In an effort to improve analytics for identifying and blocking fraudulent and unwanted calls, the Consumer Complaint Data[53] Center supports batch data downloads and graphs.

[50] YouMail, "The Robocaller Who Cried 'Wolf!'" October 6, 2020, https://blog.youmail.com/2020/10/the-robocaller-who-cried-wolf/.

[51] YouMail, "Robocall Index," https://robocallindex.com.

[52] Federal Communications Commission, "Consumer Complaint Center," https://consumercomplaints.fcc.gov/hc/en-us

[53] Federal Communications Commission, "Consumer Complaint Data Center," https://www.fcc.gov/consumer-help-center-data

9.3 FTC CONSUMER COMPLAINT DATABASE

The FTC publishes records of consumer do-not-call (DNC) complaints on its website and avia a periodic data book. The FTC received a record number of complaints (7 million) in 2017 compared to a relatively stable number of complaints in 2016 and 2018-2020 (5 million per year). Figures 9.2-9.3 provide highlights from the FTC records.[54]

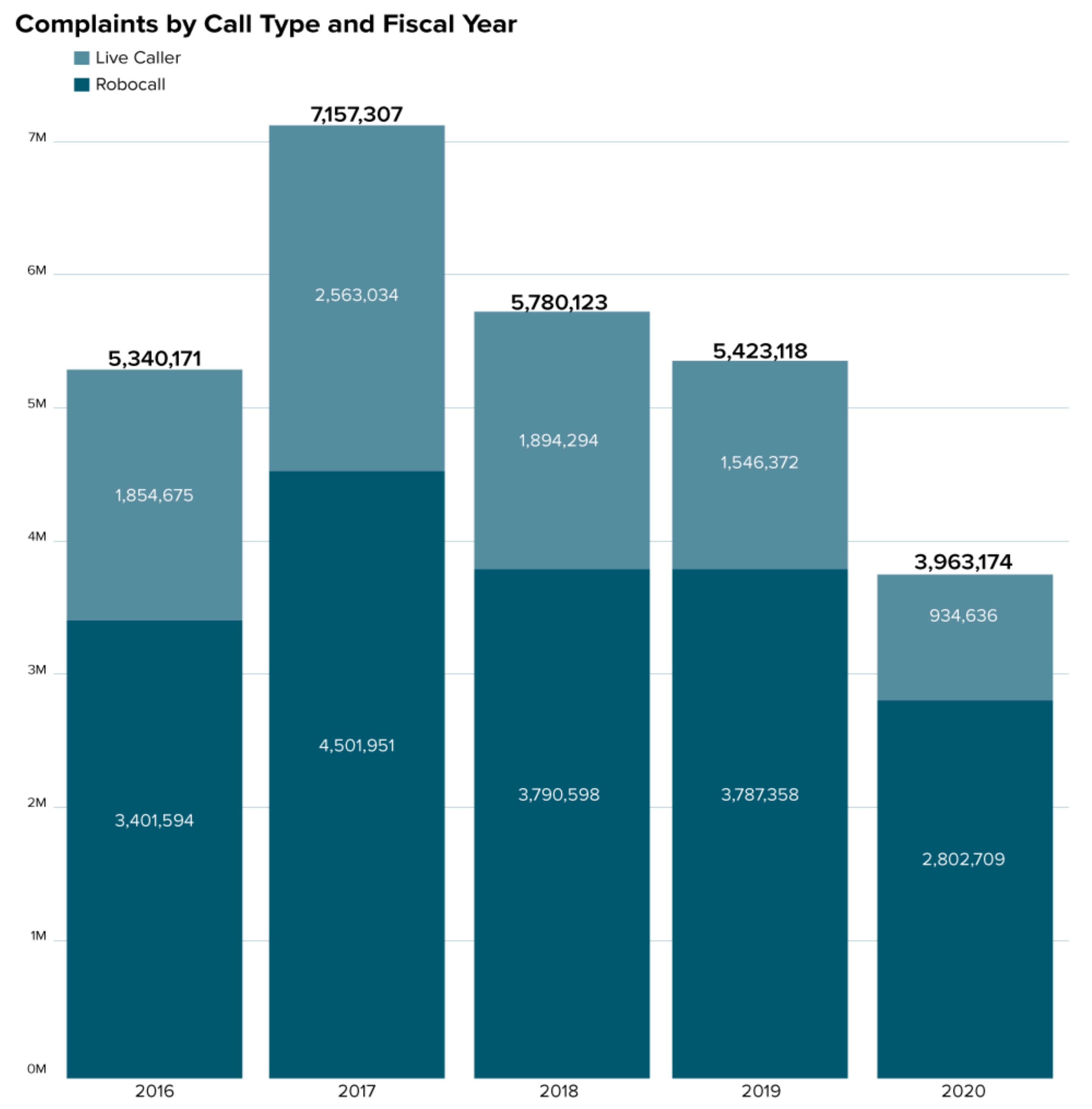


Figure 9.2: FTC Complaints by Call Type by Year [55]

[54] Federal Trade Commission, Do Not Call Data Book 2020, October 2020, https://www.ftc.gov/system/files/documents/reports/national-do-not-call-registry-data-book-fiscal-year-2020/dnc_data_book_2020.pdf.

[55] Ibid.

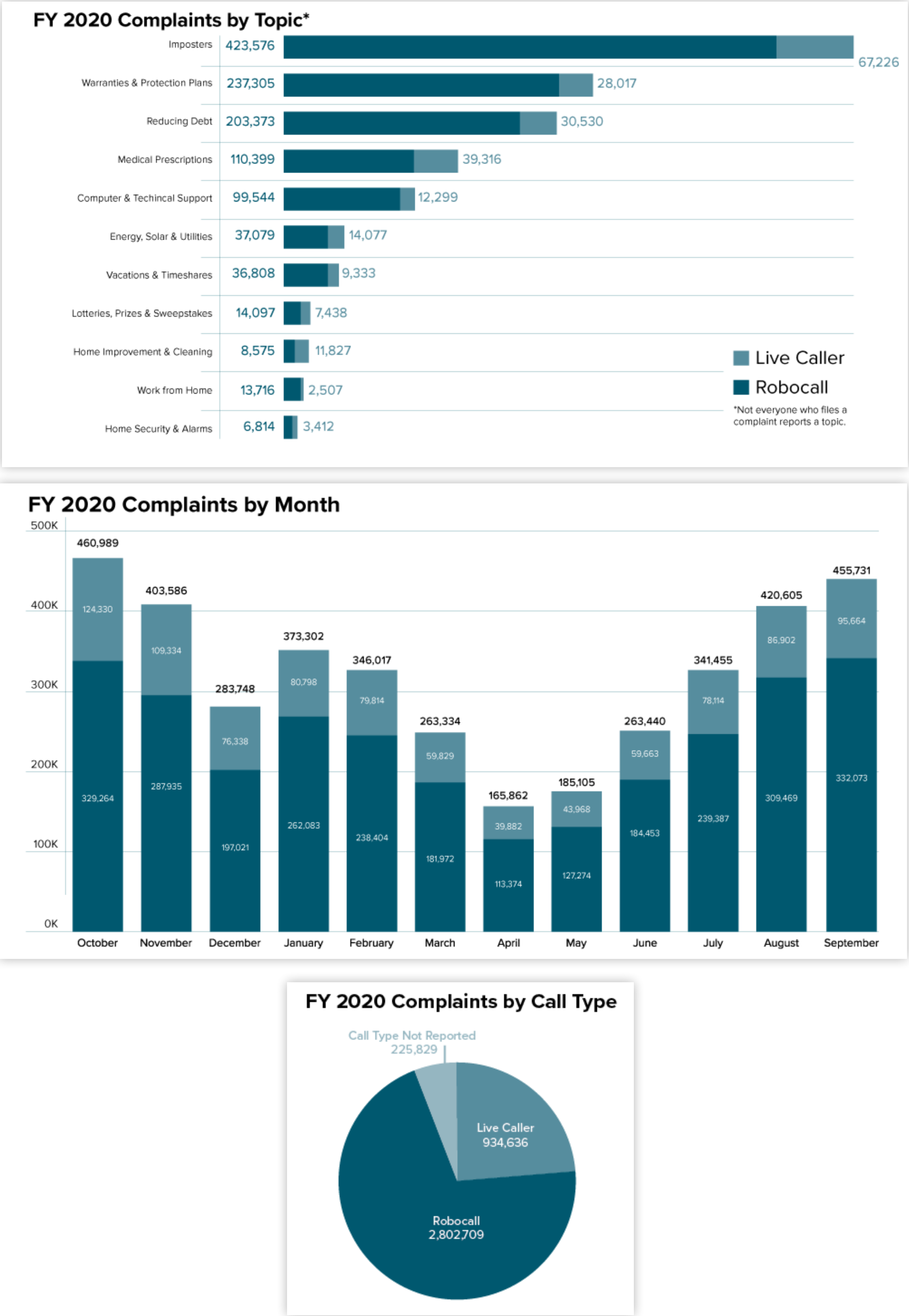


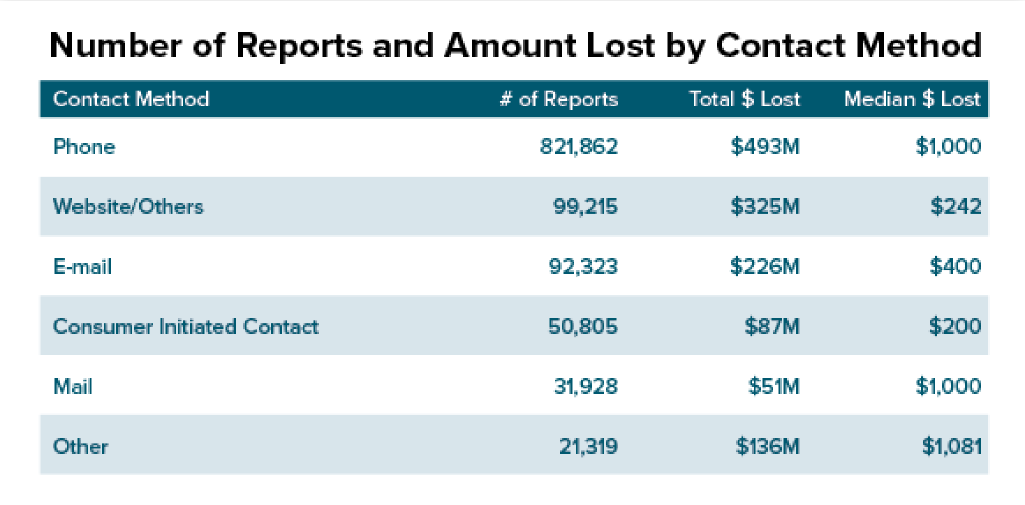
Figure 9.3: October 2019 - September 2020 Complaints by Month by Call Type[56]

[56] Ibid.

Based on the direct consumer complaints that the FCC receives, as of October 2020, robocalls account for 72.9% of call complaints relative to live callers. The top complaint type is calls from imposters impersonating brands or enterprises when they call those consumers.

9.4 FINANCIAL IMPACT

The FTC measures and publishes reports and losses by consumers and makes the data available in the FTC Consumer Sentinel Data Book. As Figure 9.4 shows, in 2019, the FTC Consumer Sentinel Databook reported 821,826 reports of initial contact by phone call and $493 million in consumer losses.[57]



Number of Reports and Amount Lost by Contact Method

Contact Method	# of Reports	Total $ Lost	Median $ Lost
Phone	821,862	$493M	$1,000
Website/Others	99,215	$325M	$242
E-mail	92,323	$226M	$400
Consumer Initiated Contact	50,805	$87M	$200
Mail	31,928	$51M	$1,000
Other	21,319	$136M	$1,081

Figure 9.4: Number of Reports and Consumer Amount Lost by Contact Method

To estimate overall financial damages to consumers, TrueCaller conducted a phone scam survey via the Harris Poll in March 2020 of 2,024 U.S. adults. Based on the 441 respondents that claimed they lost money to phone scams in the past 12 months, TrueCaller estimated nearly 1 in 4 (22% or 56 million total) of all U.S. consumers lost a total of $19.7 billion to phone scams in the prior 12-month period.[58]

9.5 CONSUMER CALL ENGAGEMENT

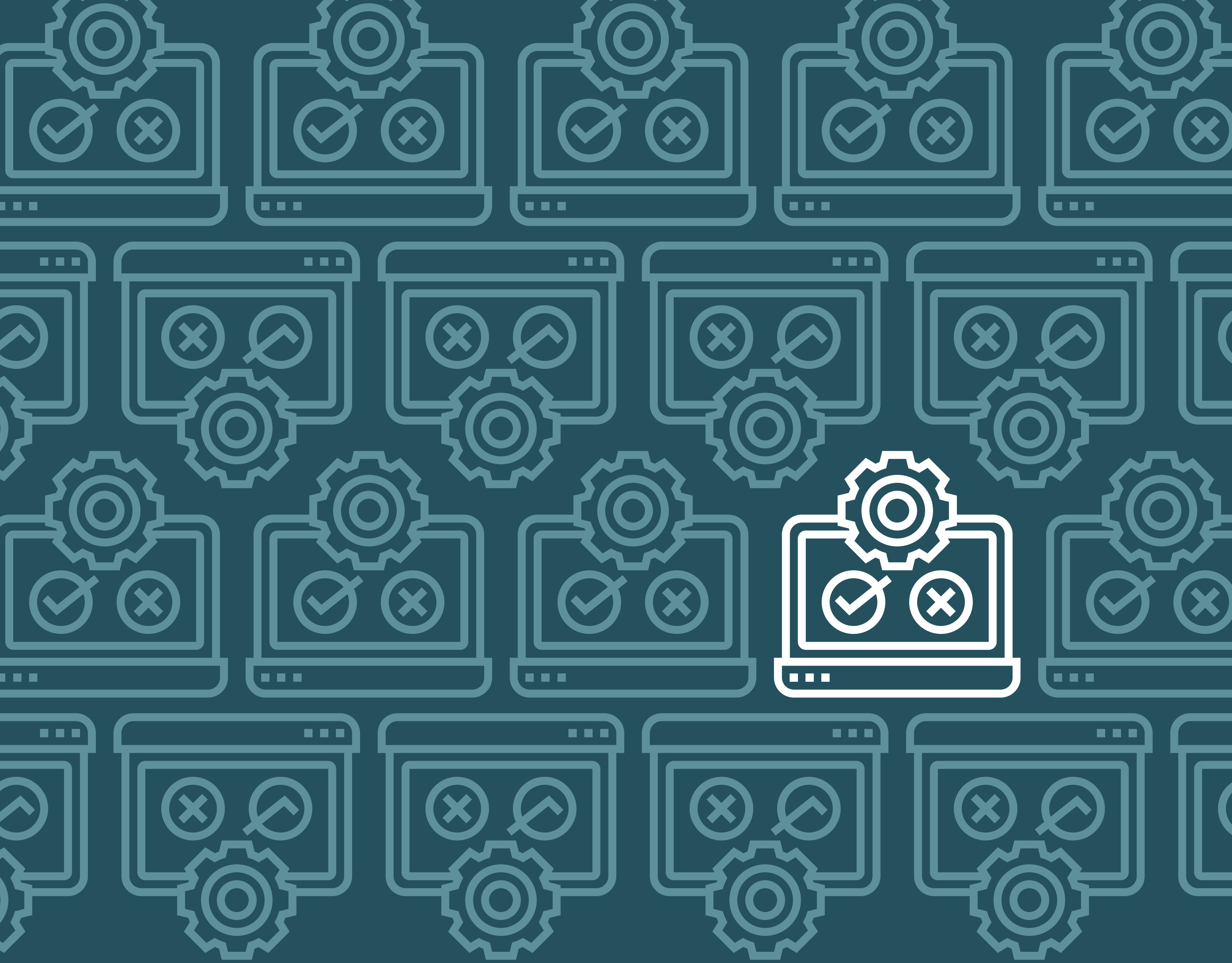
The increased volume of unwanted phone calls has taken a toll on call engagement, as well. All major call origination industries are reporting a steady decline of 20% to 30% per year[59] in call pickup rates. Currently, 76% of all calls with no identifying information (e.g., address book name or information provided by a caller ID service) are unanswered.[60]

[57] Federal Trade Commission, Consumer Sentinel Network: Data Book 2019, January 2020, https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2019/consumer_sentinel_network_data_book_2019.pdf.

[58] Truecaller, Truecaller Insights - US Spam & Scam Report 2020, April 16, 2020, https://truecaller.blog/2020/04/16/truecaller-insights-2020-us-spam-scam-report/.

[59] Numeracle, Numeracle Contact Rate Case Study, https://www.numeracle.com/resources/contact-rate-improvement-case-study

[60] Hiya, State of the Phone Call, https://blog.hiya.com/state-of-the-call-report-mobile-phones-in-the-era-of-robocalls/.



10

SUCCESS CRITERIA

10.1 GENERAL SUCCESS CRITERIA

A simple mark of success will be when the number of illicit calls is reduced to a level that customers consider acceptable on an ongoing basis, which is expected to be around zero. This reduction will be achieved when it becomes uneconomic for the spammers to carry out their illicit business.

At the same time, the successful mitigation methods must not create unacceptable degradation to the quality, utility, and economics of legitimate network use. For example, the delivery of public service robocalls and legitimate origination spoofing should not be impacted.

To understand whether the industry is making progress in stemming the robocall epidemic, the industry needs to start tracking progress. ATIS can help by defining relevant terms and recommend metrics that can help identify if the problem is getting better. ATIS can then correlate publicly available metrics with more technical metrics about whether mitigation techniques are being used.

10.2 MEASURABLE SUCCESS CRITERIA

Allowing providers to collect data based on their analytics services and deployment models would be sufficient to support an effective evaluation. However, there are critical factors that may be considered, including:

- Coverage: The number of subscribers and the types of subscribers that are benefiting from call treatment tools and services.
- Performance: The number of calls being treated and the degree of accuracy.
- Customer Satisfaction: The level of satisfaction with the performance of the mitigation tools and of efforts to bring greater transparency to “good calls.”

There are also meaningful measurement principles that may be considered, including:

- Flexibility across Tools/Solutions: Allow providers to collect different statistics for different solutions to satisfy differing subscriber preferences.
- Flexibility over Time: Allow providers to collect different statistics over time to accommodate new/changed features in their solutions because scams constantly evolve/change.
- Understand Implications: Providers should explain what the statistics mean and do not mean and revise explanations as statistics change. For example, what does “increase in calls identified as scams” mean?
    - The analytics service is improving (false negatives decreasing)?
    - The total number of scam calls is increasing?
    - The false positives are increasing?
    - Combinations of two or more of the above?

11
ROBOCALLING MITIGATION METRICS

11.1 ROBOCALL METRICS

11.1.1 Proposed Metric: Tracebacks

Number of tracebacks performed per month.

11.1.1.1 Rationale

The number of tracebacks performed highlights how the industry is taking action to mitigate robocalls. An increase in tracebacks should correlate with a reduction of reported robocalls. In 2019, Industry Traceback Group reported conducting more than 1,000 tracebacks, implicating more than 10 million robocalls.

11.1.1.2 Source of Metric

Industry Traceback Group.

11.1.2 Proposed Metric: FCC Robocalling Complaints

Number of robocalling complaints to the FCC broken down in the collected categories: unwanted calls, telemarketing (including do-not-call and spoofing), and robocalls.

11.1.2.1 Rationale

Unwanted calls, including illegal and spoofed robocalls, are the FCC's top consumer complaint, with over 200,000 complaints each year, around 60% of all the complaints that the FCC receives. It was estimated that U.S. consumers received nearly 4 billion robocalls per month in 2018. These include complaints from consumers whose numbers are being spoofed or whose calls are being mistakenly blocked or labeled as a possible scam call by a robocall blocking app or service. If robocall mitigation is successful, FCC consumer complaints should trend down.

11.1.2.2 Source of Metric

FCC.[61]

11.1.3 Proposed Metric: FTC DNC Complaints

DNC complaints to the FTC per month broken down by the collected categories:

- Calls pretending to be government, businesses, or family and friends
- Charities
- Computer and technical support
- Dropped call or no message
- Energy, solar, and utilities
- Home improvement and cleaning
- Home security and alarms
- Lotteries, prizes, and sweepstakes
- Medical and prescriptions
- No subject provided
- Other
- Reducing your debt (e.g., credit cards, mortgage, student loans)
- Vacation and timeshares
- Warranties and protection plans
- Work from home and other ways to make money

11.1.3.1 Rationale

FTC collects DNC complaints that include unwanted calls such as telemarketing calls. In FY2019, the FTC received 5,422,298 DNC complaints. If this metric is trending down, it would indicate mitigation efforts are successful.

[61] See https://opendata.fcc.gov/Consumer/Consumer-Complaints-Data-Unwanted-Calls/vakf-fz8e.

11.1.3.2 Source of Metric

The FTC.[62]

11.2 ANALYTICS SERVICES METRICS

11.2.1 Proposed Metric: Illegal

Percentage and number of total calls identified as being illegal (and sub portion being delivered with PASSporT A).

11.2.1.1 Rationale

This would indicate how impactful analytics services are in labeling calls as illegal.

11.2.1.2 Source of Metric

TSPs (or their delegated analytics service).

11.2.2 Proposed Metric: Nuisance

Percentage and number of total calls identified as being nuisance (and sub portion being delivered with PASSporT A).

11.2.2.1 Rationale

This would indicate how impactful analytics services are in labeling calls as nuisance.

11.2.2.2 Source of Metric

TSPs (or their delegated analytics service).

11.2.3 Proposed Metric: Remediation Requests

Remediation requests for incorrect labeling by analytics services/TSPs.

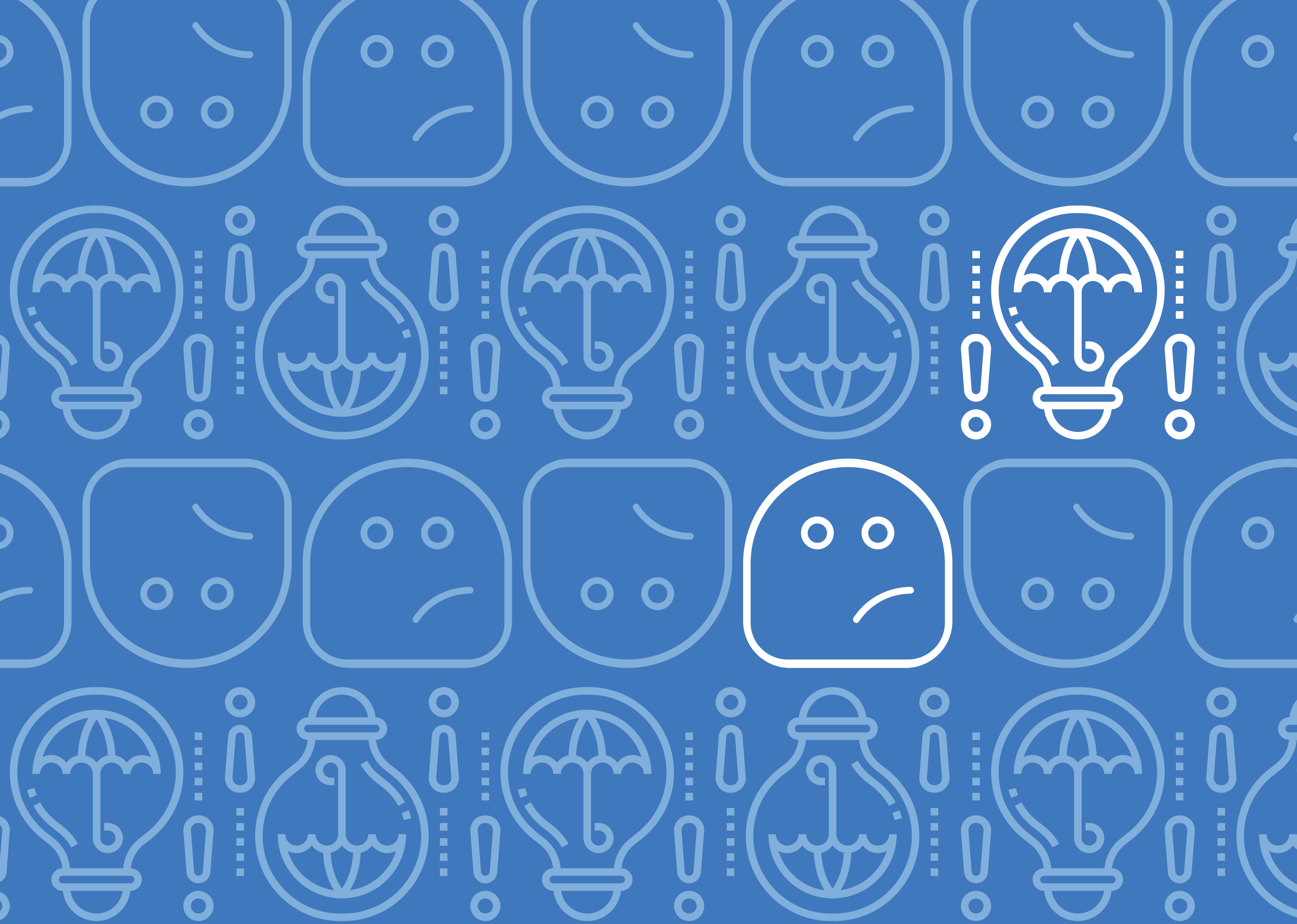
11.2.3.1 Rationale

The number of remediation requests should be inversely proportional to how "reasonable" the analytics service is.

11.2.3.2 Source of Metric

TSPs (or their delegated analytics service).

[62] See https://www.ftc.gov/site-information/open-government/data-sets/do-not-call-data.



12

UNINTENDED CONSEQUENCES AND MITIGATION AIMS

UNINTENDED CONSQUENCES AND MITIGATION AIMS

Success in reducing malicious robocalls to “acceptable” levels will place more focus on reducing what the public has long regarded as nuisance calling. Successful solutions to the current problems associated with illegal robocalling must still allow legitimate robocalls to be delivered. However, the effectiveness of those legal robocalls may have been eroded due to consumers’ negative perception of robocalls caused by the current wave of illicit robocalling.

Additionally, the tools provided to counter illegitimate calling may also be used by network users to screen out such legitimate calls. Those tools will allow pro-active enforcement of TCPA and DNC lists, likely replacing the current but less effective reactive enforcement.

A return to the status quo that existed prior to the rise of malicious robocalling may not be achievable.

Ultimately, the aim is to allow the call recipient to trust the accuracy of the information provided regarding the call. The intermediate steps towards this goal are:

1. Provide advice to recipient on likely nature of call (good/bad).
2. Block calls originating from sources likely to have bad intent.

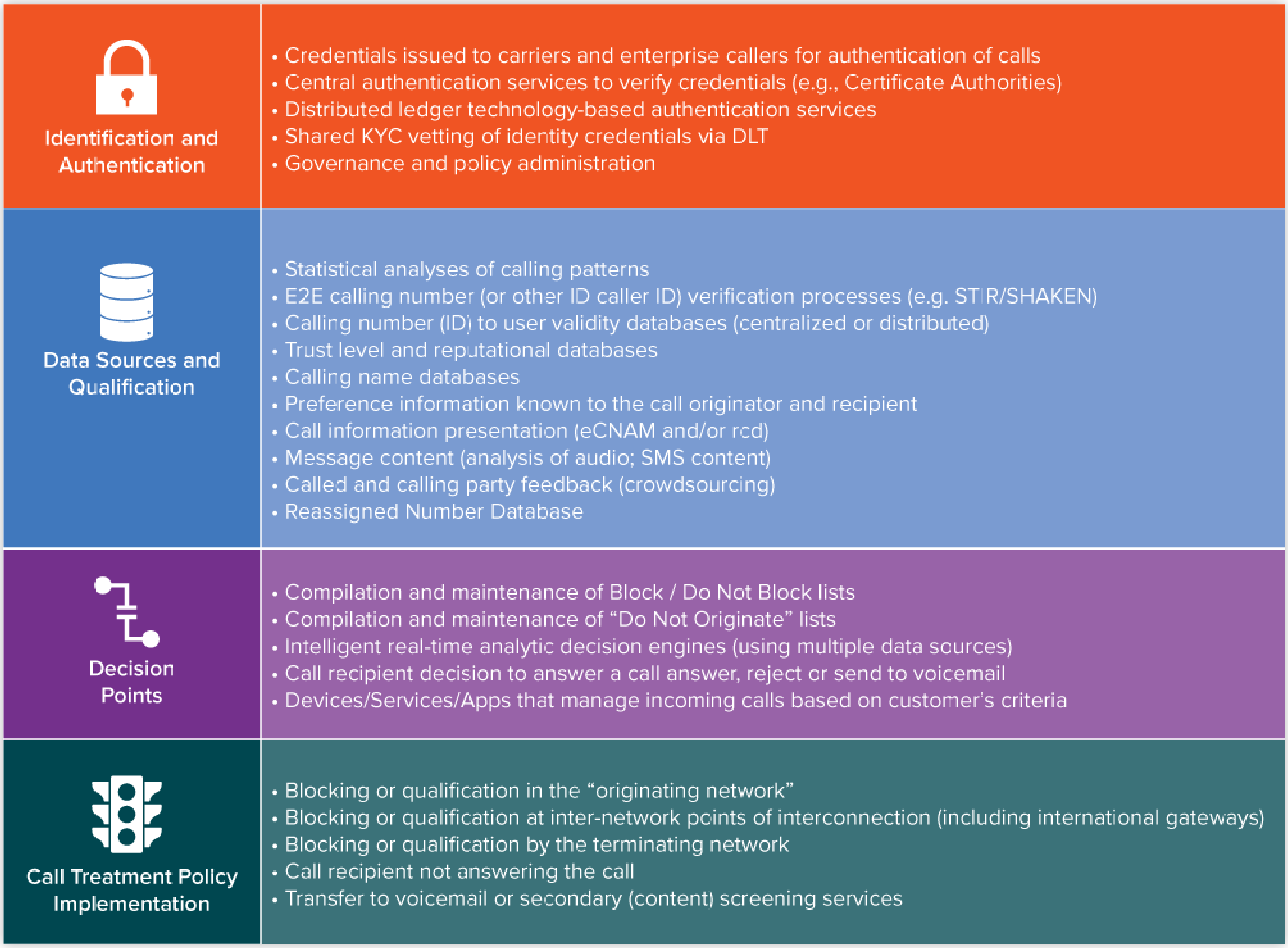
13

CATEGORIZATION AND COMBINATION OF ANTI-ROBOCALLING MITIGATION TECHNIQUES

CATEGORIZATION AND COMBINATION OF ANTI-ROBOCALLING MITIGATION TECHNIQUES

Many different component techniques exist that may be used in combination to provide illicit call mitigation services. It may not be evident to readers as to how these various techniques may be combined. This section describes a structure and methodology that enable a more straightforward comprehension of the relationships between these various component techniques, which may enable the creation of additional anti-illicit-call services.

Different industry players have attempted, individually and collectively, to combat the robocalling phenomenon since 2013. Those attempts were ineffective and revealed the need for a more concerted effort. In 2016, the FCC launched a Strike Force against robocalls, examining all the aspects deemed necessary to address the root problem rather than just its varying symptoms. After reviewing the Strike Force findings, many industry leaders in robocall mitigation concluded that no silver bullet exists to solve the illegal and unwanted robocalling problem.[63] However, the industry's collective experience pointed to the effectiveness of multilayered approaches against the ever-changing fraud landscape. This report has described various components that may be combined to reduce the level and impacts of illegal robocalling while attempting to maintain service quality for legitimate callers. These components may be characterized in the following classes:



Identification and Authentication	• Credentials issued to carriers and enterprise callers for authentication of calls • Central authentication services to verify credentials (e.g., Certificate Authorities) • Distributed ledger technology-based authentication services • Shared KYC vetting of identity credentials via DLT • Governance and policy administration
Data Sources and Qualification	• Statistical analyses of calling patterns • E2E calling number (or other ID caller ID) verification processes (e.g. STIR/SHAKEN) • Calling number (ID) to user validity databases (centralized or distributed) • Trust level and reputational databases • Calling name databases • Preference information known to the call originator and recipient • Call information presentation (eCNAM and/or rcd) • Message content (analysis of audio; SMS content) • Called and calling party feedback (crowdsourcing) • Reassigned Number Database
Decision Points	• Compilation and maintenance of Block / Do Not Block lists • Compilation and maintenance of "Do Not Originate" lists • Intelligent real-time analytic decision engines (using multiple data sources) • Call recipient decision to answer a call answer, reject or send to voicemail • Devices/Services/Apps that manage incoming calls based on customer's criteria
Call Treatment Policy Implementation	• Blocking or qualification in the "originating network" • Blocking or qualification at inter-network points of interconnection (including international gateways) • Blocking or qualification by the terminating network • Call recipient not answering the call • Transfer to voicemail or secondary (content) screening services

Figure 13.1: Component Techniques Used in Combination to Provide Illicit Call Mitigation Services

[63] Industry Robocall Strike Force Report, April 28, 2017, https://www.fcc.gov/file/12311/download.

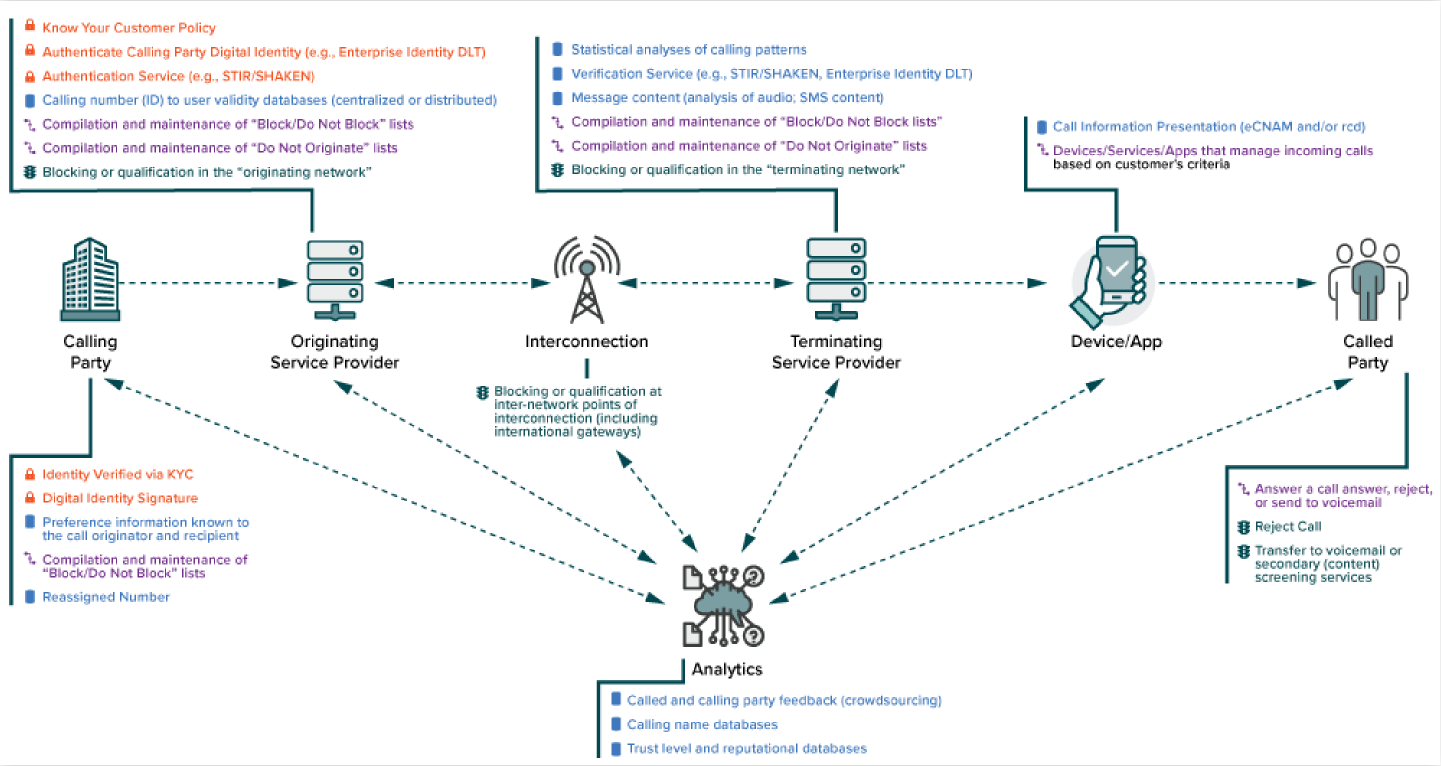
Mitigation capabilities/services typically use multiple data sources and have multiple decision points cascaded. Each decision point in the chain considers both the output from the upstream decision point and additional data that may be context specific. For example, a network-based screening service may take input from both number reputation services and STIR/SHAKEN and determine that a call may be legitimate but passes all the call data to the recipient. The recipient may determine otherwise and reject the call based on their own knowledge of issues with calls from the identified party.

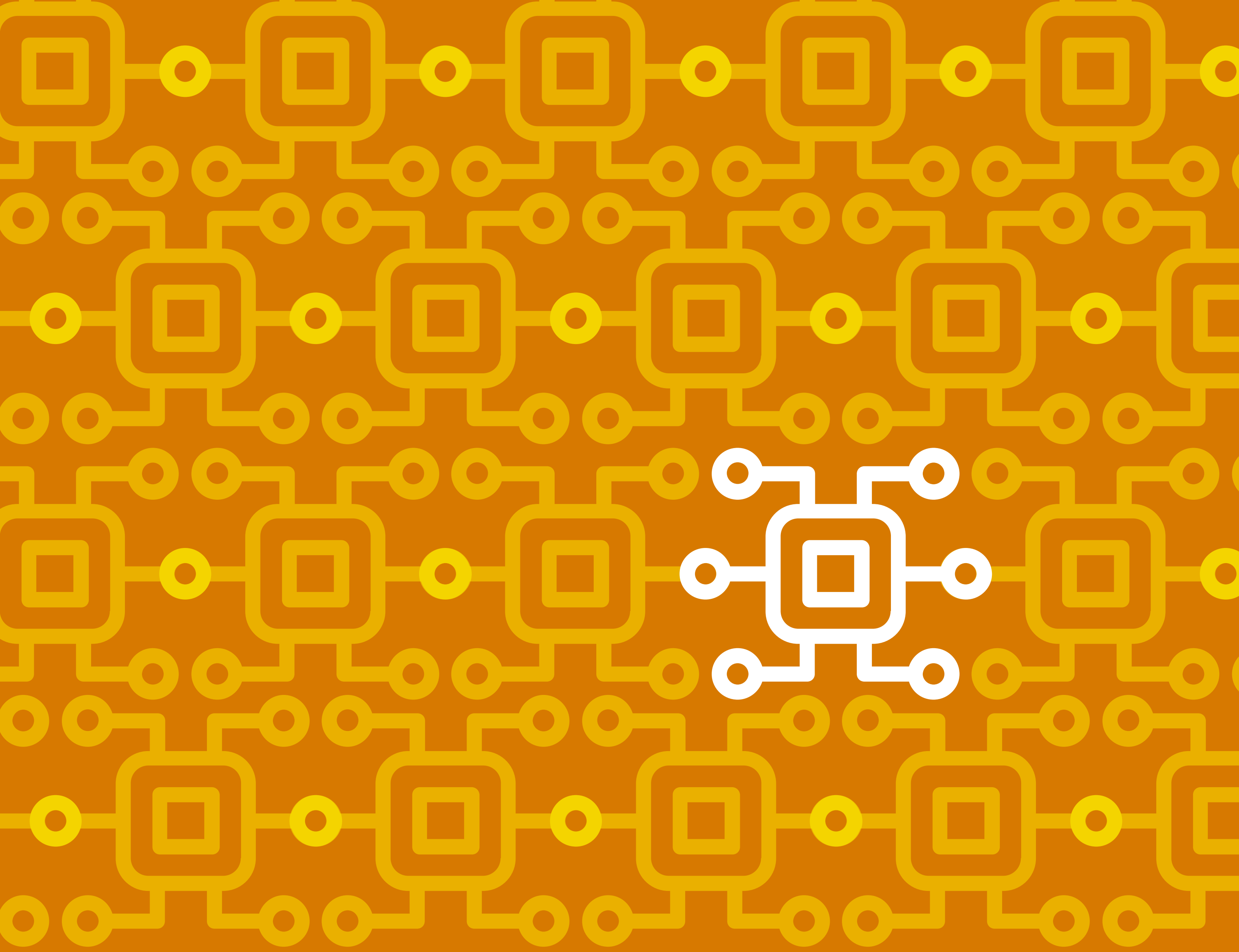
In this new network, each call will encounter a different set of treatments depending on the call's origin and destination, the reputation, and analytics available at the terminating end, and the services/devices used by the called party. Figure 13.2 illustrates some of the more common components (from the above lists) brought together to protect the called party at each stage of a call.

Note that by considering this structure, the industry can learn how competition has been enabled in the provision of robocalling mitigation services. Even with a common set of data inputs available (e.g., multiple industry-wide block/allow lists and ID reputation ratings, STIR/SHAKEN results), the use of proprietary decision engines and the various call treatments used by each service collectively allow a range of offerings to be developed, from which customers may choose whichever best meets their needs.

While carriers were tasked with complex technical solutions, regulators provided clear guidelines and requirements to facilitate the reduction of robocalls. Regulatory support may not be viewed as a component like the ones described above. However, it effectively created the legal landscape to enable all the above industry solutions. Section 18 offers a comprehensive summary of the government's regulatory actions to curb robocalls thus far.

Figure 13.2: Example Mitigation Components Used at Each Call Stage


Know Your Customer Policy
Authenticate Calling Party Digital Identity (e.g., Enterprise Identity DLT)
Authentication Service (e.g., STIR/SHAKEN)
Calling number (ID) to user validity databases (centralized or distributed)
Compilation and maintenance of "Block/Do Not Block" lists
Compilation and maintenance of "Do Not Originate" lists
Blocking or qualification in the "originating network"
Statistical analyses of calling patterns
Verification Service (e.g., STIR/SHAKEN, Enterprise Identity DLT)
Message content (analysis of audio; SMS content)
Compilation and maintenance of "Block/Do Not Block lists"
Compilation and maintenance of "Do Not Originate" lists
Blocking or qualification in the "terminating network"
Call Information Presentation (eCNAM and/or rcd)
Devices/Services/Apps that manage incoming calls based on customer's criteria
Calling Party
Originating Service Provider
Interconnection
Terminating Service Provider
Device/App
Called Party
Blocking or qualification at inter-network points of interconnection (including international gateways)
Identity Verified via KYC
Digital Identity Signature
Preference information known to the call originator and recipient
Compilation and maintenance of "Block/Do Not Block" lists
Reassigned Number
Answer a call answer, reject, or send to voicemail
Reject Call
Transfer to voicemail or secondary (content) screening services
Analytics
Called and calling party feedback (crowdsourcing)
Calling name databases
Trust level and reputational databases



14
MITIGATION COMPONENTS IN USE OR IN DEVELOPMENT

14.1 STIR/SHAKEN – SP-TO-SP VERIFICATION

STIR/SHAKEN is a framework of interconnected standards that enables SP-to-SP verification of the caller ID. It enables calls traveling through interconnected IP phone networks to have their caller ID "signed" as legitimate by originating carriers and validated by other carriers before reaching consumers. STIR/SHAKEN digitally validates the handoff of phone calls passing through the complex web of IP networks, allowing the phone company of the consumer receiving the call to verify that a call is in fact from the number displayed on caller ID.

14.1.1 History

The FCC has been leading the push for industry adoption of standards to help consumers as quickly as possible. The Commission prompted real progress in call authentication by starting a formal inquiry in July 2017, seeking public input about the best way to establish a reliable system to verify the caller ID information that appears on the recipient's phone. This FCC inquiry resulted in a North American Numbering Council-recommended framework for implementing an industry-developed standard to help prevent illegal attempts to trick consumers through caller ID spoofing. STIR/SHAKEN should establish a reliable authentication system that will help strengthen call-blocking services and unmask spoofed calls.

In November 2018, the FCC demanded that the phone industry adopt a robust call authentication system to combat illegal caller ID spoofing and implement that system within a year. FCC Chairman Pai sent letters to the major voice providers asking them to outline their plans to protect their customers and implement the STIR/SHAKEN standards—and do so without delay. In February 2019, the FCC welcomed many carriers' commitments to meeting his timeline for implementation, called on others to "catch up," and made clear that the FCC would consider regulatory intervention if necessary. In June 2019, the Commission adopted a Notice of Proposed Rulemaking, which positions the agency to mandate the implementation of the STIR/SHAKEN caller ID authentication framework if the end-of-the-year deadline is not met, allowing the FCC to move directly to final rules if needed.

14.1.2 Application

STIR[64] is a set of technical standards developed by the Internet Engineering Task Force (IETF) to verify the calling party is authorized to use a particular TN. STIR does not define how carriers should deploy the standards to mitigate illegitimate calls.

The SHAKEN framework establishes an end-to-end architecture that allows an OSP to authenticate and assert a telephone identity and provides for the verification of this telephone identity by a TSP. The SHAKEN framework defines a profile, using protocols standardized in the IETF STIR Working Group.

SHAKEN uses a trusted public key infrastructure to enhance the integrity of the originating call identifying data sent across networks. SIP headers will contain a level of confidence indicator from the OSP to signal whether the party originating the call has the right to use the number via the attestation field. There are three levels of attestation that can be indicated by the OSP:

- Full Attestation: The SP has authenticated its customer originating the call and it is authorized to use the calling number.
- Partial Attestation: The SP has authenticated its customer originating the call but can't verify that it is authorized to use the calling number.
- Gateway Attestation: The SP has authenticated from where it received the call, but can't authenticate the call source (e.g., international gateway call).

In addition to the attestation level, the OSP provides data in the header to facilitate traceback identifying where the call entered their network.

14.1.3 Scope

STIR/SHAKEN does not prevent unwanted robocalls by itself. Instead, it helps mitigate caller ID spoofing. There are other call analytics techniques designed to prevent robocalls, but they are less effective when the calling number has been spoofed.

Effective robocall prevention requires both STIR/SHAKEN to check for spoofing and call analytic services,

[64] IETF, "STIR into Action," January 6, 2020, https://www.ietf.org/blog/stir-action/.

which are much more effective when you know whether the calling number is spoofed. Other mitigation techniques and their use in combination with STIR/SHAKEN are described later in this report.

In addition, the following issues limit the effectiveness of STIR/SHAKEN:

- Non-IP networks (e.g., Time Division Multiplexing (TDM)) cannot transmit the identity header.
- Some SIP network gear removes the identity token.
- Some SIP networks use User Datagram Protocol (UDP), which is prone to packet loss and fragmentation.

If a call transfers to TDM interconnect at any time, the signed token will be lost, along with the ability to authenticate the caller ID.

Robocalls that originate on VoIP networks often end up traversing the PSTN because providers are typically limited to interconnects between large carriers.

There is also a problem of added costs for the smaller carriers. Smaller providers that have earlier generation, non-IP equipment may not have the resources to allocate for implementation.

14.2 STIR/SHAKEN ROLLOUT METRICS

14.2.1 Proposed Metric: Active SPs

Number of SPs signed-up in relation to the number of eligible providers.

14.2.1.1 Rationale

Provides an understanding of adoption of STIR/SHAKEN by SPs.

14.2.1.2 Source of Metric

STI-PA/GA.

14.2.2 Proposed Metric: TSP Calls

Percentage of TSP calls that were delivered with SHAKEN PASSporTs. Broken down by attestation level (A/B/C).

14.2.2.1 Rationale

This metric would indicate the efficacy of STIR/SHAKEN roll-out.

14.2.2.2 Source of Metric

Any TSP.

14.2.3 Proposed Metric: Inter-SP Calls Terminating at a TSP

Percentage of inter-SP calls with SHAKEN PASSporTs terminating at a TSP.

14.2.3.1 Rationale

This metric would indicate the exchange of SHAKEN PASSporTs between SPs. While the previous metric would include intra-SP signed calls, this would indicate whether the SP community is exchanging signed traffic.

14.2.3.2 Source of Metric

Any TSP.

14.2.4 Extensions to STIR/SHAKEN

STIR/SHAKEN is applicable only to networks using end-to-end IP. For non-IP networks, alternative solutions are being created to provide SP-to-SP verification of the caller ID. As with STIR/SHAKEN, the outputs of this verification may be used as data input to the decision process(es) that determine the treatment of a call.

14.2.4.1 STIR Out-of-Band (OOB), SHAKEN Out-of-Band

On March 10, 2020, the FCC issued a Report and Order and Further Notice of Proposed Rulemaking that took a critical step in the Commission's multi-pronged approach to ending illegal caller ID spoofing by requiring voice SPs to implement caller ID authentication technology.[65]

The Proposed Rulemaking would require originating and terminating voice SPs to implement the STIR/SHAKEN caller ID authentication framework in the IP portions of their networks by June 30, 2021. This deadline is consistent with the TRACED Act recently passed by Congress.

The rulemaking requires voice SPs using non-IP technology to either upgrade their networks to IP to enable STIR/SHAKEN implementation or work to develop non-IP caller ID authentication technology and implement a robocall mitigation program in the interim.

Currently, SPs negotiate network interconnect agreements among themselves that describe the price they will pay to have their calls sent through the network. They use routing software to select available routes based upon quality and price, which may lead to extended call paths as calls travel from one carrier to the next. Extended call paths increase the risk that the Identity token may be lost in transit.

Because STIR/SHAKEN only operates on IP networks, some stakeholders have advocated for a solution referred to as "Out-of-Band (OOB) STIR." With OOB STIR, the caller ID authentication information is sent across the internet, out-of-band from the call path, allowing STIR/SHAKEN to be implemented on networks that are not fully IP.

The IETF Network Working Group has been developing draft use cases for STIR OOB.[66] It recognizes that not all telephone calls currently use SIP. However, even those using SIP do not always carry SIP signaling end-to-end. Calls from TNs still routinely traverse the PSTN at some point. Broadly, calls fall into one of three categories:

- One or both of the endpoints is actually a PSTN endpoint.
- Both endpoints are non-PSTN (SIP), but the call transits the PSTN at some point.
- Non-PSTN calls that do not transit the PSTN at all (e.g., native SIP end-to-end calls).

The ATIS Packet Technologies and System Committee (PTSC) launched the Non-IP Call Authentication (NIPCA) Task Force in June 2020.[67] NIPCA will identify and document call authentication challenges facing TDM networks, investigate the feasibility of potential solutions in this area, and evaluate the implementation viability of TDM call authentication frameworks. NIPCA is currently progressing work in this area. ATIS provided an update to the Commission on October 27, 2020, about NIPCA's work to update call authentication issues.[68]

14.2.5 Complementary Approaches for "Trusted Caller Origination"

There are use cases where a SHAKEN OSP may not have complete locally available information to establish a verified association between a calling TN and its direct customer. Without the verified association, there is no basis for assigning a "full attestation" value to particular calls.

In addition, Delegated Certificates, Extended Validation (EV) Certificates with TN Letter of Authorization (LOA), and Central Database are proposed mechanisms for providing OSPs with additional information about the entity placing a call and the TNs with which an entity has a valid association. This information would help OSPs mark each call with the highest attestation level. All three approaches are considered viable. However, they do present different tradeoffs in terms of complexity, cost to SPs and enterprises, and the assumptions around the relationship between SPs, their customers, and other entities in the SHAKEN and voice network ecosystems. It is difficult to predict how these tradeoffs will influence industry acceptance of one solution over another. It is likely that the "best" solution will vary based on the deployment use case.

Identification and Authentication

14.2.5.1 Delegated Certificates

Three sub-options have been presented for passing vetted enterprise call origination information in the SIP signaling flow to enable an OSP to assign A-level attestation to enterprise-originated calls: Delegated Certificates, Lemon Twist, and Enterprise Certificates. All three extend the baseline SHAKEN framework to allow for an additional SIP Identity header field added by the enterprise as a mechanism for passing required enterprise call origination information to the OSP ("enterprise signature"). The three solutions suggest several different options that the industry can use to issue Security Telephone Identity (STI) certificates to vetted enterprise customers. Once an enterprise has obtained an STI certificate, the three implementation models are nearly identical.

[65] Call Authentication Trust Anchor, WC Docket Nos. 17-97 and 20-67, Report and Order and Further Notice of Proposed Rulemaking, 2020.

[66] IETF, draft-ietf-stir-oob-07, https://datatracker.ietf.org/doc/draft-ietf-stir-oob/.

[67] ATIS, "Non-IP Call Authentication Task Force," https://www.atis.org/committees-forums/ptsc/non-ip-call-authentication-task-force/.

[68] Alliance for Telecommunications Industry Solutions to Marlene H. Dortch, "Re: WC Docket No. 20-323," Ex Parte, October 27, 2020, https://prodnet.www.neca.org/publicationsdocs/wwpdf/102820atis.pdf.

Identification and Authentication

14.2.5.2 EV Certificates with TN Letter of Authorization (LOA)

The entity asserting the use of a calling TN is either directly known via a customer's User Network Interface (UNI) identity/authentication at the OSP or is identified by a "User Identity" header whose signature is tied to EV credentials. The calling entity's real-world legal identity is vetted by a Certificate Authority (CA) that performs the EV procedure and is contained in the subject of its certificate. The CA does not necessarily need to be an STI-CA because the certificate does not by itself convey TN authorization information. The OSP determines the TN authorization by a local authorization database populated from TN LOA electronic documents (TNLoA) exchanged with the TN SP (TNSP) or through local assignments. The authorization record is tied to the EV identity and the customer whose UNI the calling entity has been allowed to use. The calling entity's identity is exposed in its certificate or is known as the direct customer of the OSP for audit and traceback purposes.

Data Sources and Qualification

14.2.5.3 Central Database

A database of TNs is provided by a central authority, although multiple agencies could provide access to this Central TN Database (CTND). The CTND's role is serving as an authoritative source of TN-to-enterprise association, including delegated authority by enterprises (e.g., to call centers). It is envisaged that the CTND has a RESTful API that is accessed by carriers (as their role as TNSPs, OSPs, etc.) but does not need to be accessed by enterprises. The database is updated by a TNSP when an enterprise requests a set of TNs. An OSP accesses the TN-to-enterprise mapping to confirm that an enterprise has permission to use a particular TN on an outbound call, and therefore that the number has been registered as "in use" by that enterprise by a valid TNSP. Each enterprise must have a unique ID by which it is known by the TNSPs and OSPs. The Enterprise ID is managed and allocated by the CTND.

Identification and Authentication

14.2.5.4 Enterprise Identity Authenticated using Distributed Ledger

Another complementary approach involves providing an Enterprise Identity implemented on a distributed ledger using digital identities to enhance the capability for STIR/SHAKEN attestation of enterprise calls in the complex call scenarios described above. The ATIS Distributed Ledger Technology (DLT) focus group has been developing a proof of concept focused on providing SPs with a better mechanism to validate that calling parties are entitled to use the TN they are using.

The Enterprise Identity Network solution leverages DLT and its cryptographic principles to provide digital identities for businesses. An enterprise's digital identity implemented using distributed identities according to the W3C Distributed Identity (DID) specification,[69] is used to authenticate the calls it makes. An enterprise is first vetted through a KYC process to authorize its digital identity. Once an enterprise has been vetted and has a DID on the distributed ledger, it can request the allocation of a TN from a TN provider indicating the purpose and intended use of the number. These TN allocations are recorded on the ledger, ensuring all stakeholders connected to the Enterprise Identity Network instantly know who has the authoritative right to place calls using this TN and for what purpose.

Using its DID, a KYC-vetted enterprise will sign originating phone calls using the SIP Identity header. These signatures enable any OSP connected to the Enterprise Identity Distributed Ledger Network to verify the calling enterprise's DID and prove that a "trusted" business is placing the call. Using this proof of identity, the OSP can then verify that the originating TN used by the enterprise has the authoritative right to use it by checking the verifiable TN credential on the Enterprise Identity Distributed Ledger Network. OSPs are thus enabled to authenticate an Enterprise Identity and prove that it is entitled to make calls from the calling TN. With this proof of identity and the number being used, the OSP can attest to the call using STIR/SHAKEN. Figure 14.1 illustrates this process.

[69] W3C, Decentralized Identifiers (DIDs) v1.0, Working Draft 20, December 2020, https://www.w3.org/TR/did-core/.

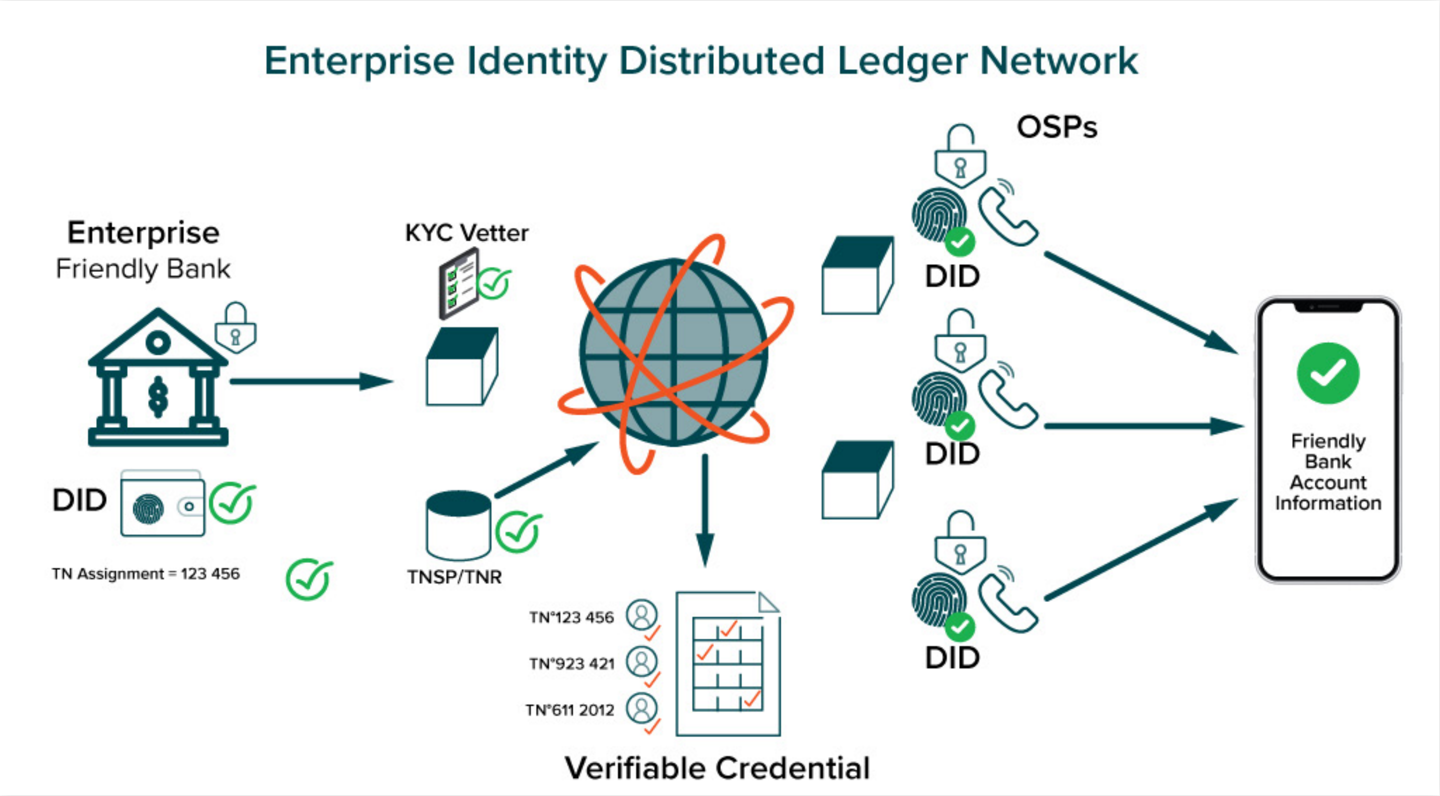


Figure 14.1: ATIS Enterprise Identity Distributed Ledger Network

For a more detailed description of the Enterprise Identity Distributed Ledger Network solution, please refer to ATIS-I-0000076, Enterprise Identity on Distributed Ledger for Authenticated Caller Use Cases.[70]

[70] ATIS-I-0000076, Enterprise Identity on Distributed Ledger for Authenticated Caller Use Cases, December 2019, https://access.atis.org/apps/group_public/download.php/50787/ATIS-I-0000076.pdf.

15

ADDITIONAL TOOLS TO HELP COMBAT ROBOCALLS

Data Sources and Qualification

15.1 REPUTATION COMPILED FROM MULTIPLE EXISTING SOURCES

Robocall analytics services, now widely deployed by carriers and technology companies alike, alert consumers to potential robocalling and spam activity so they can better assess whether to answer a call. At the same time, there is always room for improvement. For example, consumers have reported missing important and/or wanted automated calls from their children's school, their physician or pharmacy, or their financial institution. This situation occurs when an analytics service is unaware of the identity of the caller and instead relies upon call volumes and publicly generated information (e.g., crowdsourced data). Although these inputs are key to any analytics service, an understanding of the call originator's intent remains a critical factor. Carriers and analytics services must carefully balance consumer protection with ensuring legitimate businesses are not impeded from reaching their customers. The most successful balance is achieved by incorporating stringent KYC vetting, onboarding, and analytics services.

As robocall analytics services continue to be refined, businesses that suspect their TNs are being erroneously labeled or blocked do have recourse. Carriers offer websites and helplines for legitimate businesses to appeal TNs they believe are being labeled or blocked erroneously. For larger enterprise dialers whose calls traverse multiple carrier networks, there are also Aggregators offering solutions to streamline the management of appeals across multiple carriers. Calls from high-volume dialers such as schools, pharmacies, or financial institutions may now be presented to consumers, allowing them to decide whether to pick up the call.

Data Sources and Qualification

Decision Points

15.2 DATA COLLECTION AND ANALYSIS

Nearly every robocall analytics service operates through the analysis of data collected about a calling number over time. This information enables the analytics service to distinguish fraudulent or nuisance calling behavior from legitimate call traffic. In general, this information may be divided into several distinct information sets:

Phone number intelligence: The rudimentary collection of information about a phone number in isolation of any activity. For example, country of origin, number validity, allocation status, and allocated carrier.

Call traffic trends: A collection of data intelligence about the calling patterns of the phone number, including call volume, inbound-to-outbound ratios, calling times-of-day or days-of-week trends, etc. This may include historical trends of network signals such as typical STIR/SHAKEN status.

Call recipient response trends: Information about how call recipients respond to the calls generated by the originating TN. This includes pickup rates, callback rates, call duration, and out-of-band recipient reaction such as blocking future calls from the number or reporting the number to their analytics service as unwanted.

Real-time call intelligence: For more sophisticated analytics services, the service will consider details that apply only to a current phone call in real time when determining a call disposition. This may include details such as the relationship between the calling and called party TNs (e.g., neighbor calling), the current day and time, and SIP-based network signals, including STIR/SHAKEN status.

Call content: If available, a call's audio content may be considered to match the audio against known robocall campaigns or for call keywords. This analysis may be done using real-time call audio or voicemail recordings.

Registered Entity Data: Whether through a third-party registry or directly to an analytics service, entities such as government, healthcare, financial, commercial, debt collection, and utilities can attempt to register their outbound numbers along with the intent of calls. This information will be considered for inclusion in analytics to reduce false positives.

In general, the more data available to analytics services to perform their analysis, the lower the overall service error rate for both false negatives (missed spam calls) and false positives (wrongly flagged legitimate calls). This data is in addition to Do-Not-Originate lists, etc.

Data Sources and Qualification

15.3 TRACEBACK

Suspected illegal robocalls can be traced back to the call's source or traced forward to identify the entity associated with a call back number.

The traceback process traces a suspected illegal robocall to its source, even if the calling number is spoofed. When a call traverses multiple providers' networks, the process begins with the voice SP that terminated the suspected illegal robocall. Then the call is systematically traced back chronologically from provider to provider. When successful, a traceback can provide information about the originating individual or organization, the SP that originated the call, and the U.S. Point of Entry (U.S. PoE) that allowed the call onto the U.S. PSTN. At times, tracebacks are not completed because providers in the call path are not cooperative or non-responsive. Also, providers sometimes cannot find their records for the call.

The Industry Traceback Group, led by USTelecom, conducts tracebacks on behalf of the industry through a Secure Traceback Portal.[71] The Industry Traceback Group traceback process automatically generates and sends email notifications to upstream providers that fall within the call path. When the Industry Traceback Group process identifies the originator of suspicious robocalls, or a U.S. PoE routinely responsible for bringing illegal traffic into the United States, the Industry Traceback Group team asks the originator to make efforts to mitigate the illegal traffic. These mitigations include stopping the traffic and enhancing KYC measures going forward. When that traffic goes unmitigated, USTelecom may provide information to downstream carriers, as well as appropriate enforcement agencies, about the source of the illegal traffic.[72]

A trace forward is intended to address a scam that solicits a victim to call back to complete an attempted scam or fraud. In the trace forward process, the networks used to initiate the suspected call to the recipient are not traced. Instead, the network serving the callback TN is identified. The Industry Traceback Group also conducts trace forwards on behalf of the industry by contacting the voice SP that owns the DID number and requesting information about the customer with whom the number is associated.[73]

Decision Points

15.4 CALL BLOCKING (ORIGINATION, TRANSIT, AND TERMINATION)

Call blocking capabilities, which can be implemented by an SP or by a mobile device (either by the operating system (OS) natively or in conjunction with a mobile application), are available to both enterprises and consumers to help mitigate the delivery of fraudulent or other nuisance calls.

Consumers are empowered by capabilities provided by SPs (e.g., AT&T, T-Mobile), mobile OS vendors (e.g., Apple, Google), and mobile applications (e.g., Nomorobo, Hiya, PrivacyStar) to block incoming calls from either category of callers (e.g., known scammers) or specific TNs.

Call Treatment Policy Implementation

15.5 BLOCKLIST AND ALLOWLIST

Blocklisting restricts the privilege of a TN such that calls originating with the blocklisted number are typically blocked. Do-Not-Originate is where a negative reputation is associated with a TN by the SP network, resulting in SP blocking. This is a type of Blocklist. Blocklists may also be incorporated into customer provided equipment (CPE) or provided as a service feature.

There are two benefits of blocklisting TNs. First, blocklisting blocks numbers associated with known sources of illegal or unwanted calls. It may include authorization of the party with the right to use a number to block the unauthorized spoofing of the number. Second, blocklisting protects users of inward-only services such as toll-free or direct inward dialing (DID) services. The blocklisted numbers also have the potential to be ported or reassigned. Thus, these blocklisted TNs should be monitored for discontinued use and could eventually be removed from the blocklist or Do-Not Originate list.

[71] The Industry Traceback Group has been designated by the FCC as the official, single consortium that conducts private-led efforts to trace back the origin of suspected unlawful robocalls. See FCC Traceback Consortium Designation Order, DA 20-785 (rel. EB July 27, 2020), https://docs.fcc.gov/public/attachments/DA-20-785A1.pdf.

[72] USTelecom's Industry Traceback Group, Policies and Procedures, January 2020, https://www.ustelecom.org/wp-content/uploads/2020/02/USTelecom_ITG-Policies-and-Procedures_Jan-2020.pdf.

[73] Ibid.

Allowlisting lets a TN bypass call analytics services or blocking due to the accepted level of trust associated with the originating TN. The term allowlist indicates a permanent, positive reputation for a TN. However, allowlisted TNs may be spoofed, ported, or used for a new purpose. For this reason, the term is also referred to as registration. Registration allows a legitimate call originator to provide its identity details and the nature of its calls directly to carriers, analytics services, or caller identity aggregators. This registration of a number when vetted can then be taken into consideration by analytics algorithms and, in most cases, have a negative reputation removed.

Allowlisting should not be permanent. The Registry and its registered TNs should be monitored for breaches, abusive dialing practices, or suspected nefarious activity and could be assigned a negative reputation or blocklisted as a result.

Decision Points

15.6 NETWORK APPLICATIONS

Voice SPs provide several network-based services for blocking robocalls. Many of these use third-party analytics services for call blocking and labeling services of suspicious calls. Refer to Appendix A for a representative sample of the blocking services being offered currently.

15.7 PHONE AND OTHER LOCAL APPLICATIONS

15.7.1 Device Manufacturers' Blocking Services

Call Treatment Policy Implementation

Google added new features to Call Screen for its Pixel phone lineup.[74] These include the ability to detect robo- and spam calls, and then stop them from ever reaching the phone. Google Assistant will interact with the caller, and if the call turns out to be legitimate, it will route the call to the phone, along with information about the caller. Google offers several free, opt-in, call-blocking tools, such as the Phone App for Android, which provides visual warnings about a potential spam caller, enables users to block specific numbers, and allows users to report spam callers.[75]

Apple's iOS 13 added several new features, including Silence Unknown Callers, which adds the option to route calls from unknown numbers straight to voicemail. With the feature turned on, Siri will allow calls from numbers found in Contacts, Mail, and Messages to go through. Anything else will go to voicemail, and assuming the caller is legit, they can leave a message. However, people often receive important calls from numbers they do not store on their phones, so they still could miss important calls.

15.7.2 Smartphone Blocking Apps

There are a number of third-party apps available that offer automatic call blocking and spam alerts for suspicious calls and make it easy to report a number if a call slips through. Refer to Appendix B for a listing of several robocall blocking apps for iPhone and Android.

Data Sources and Qualification

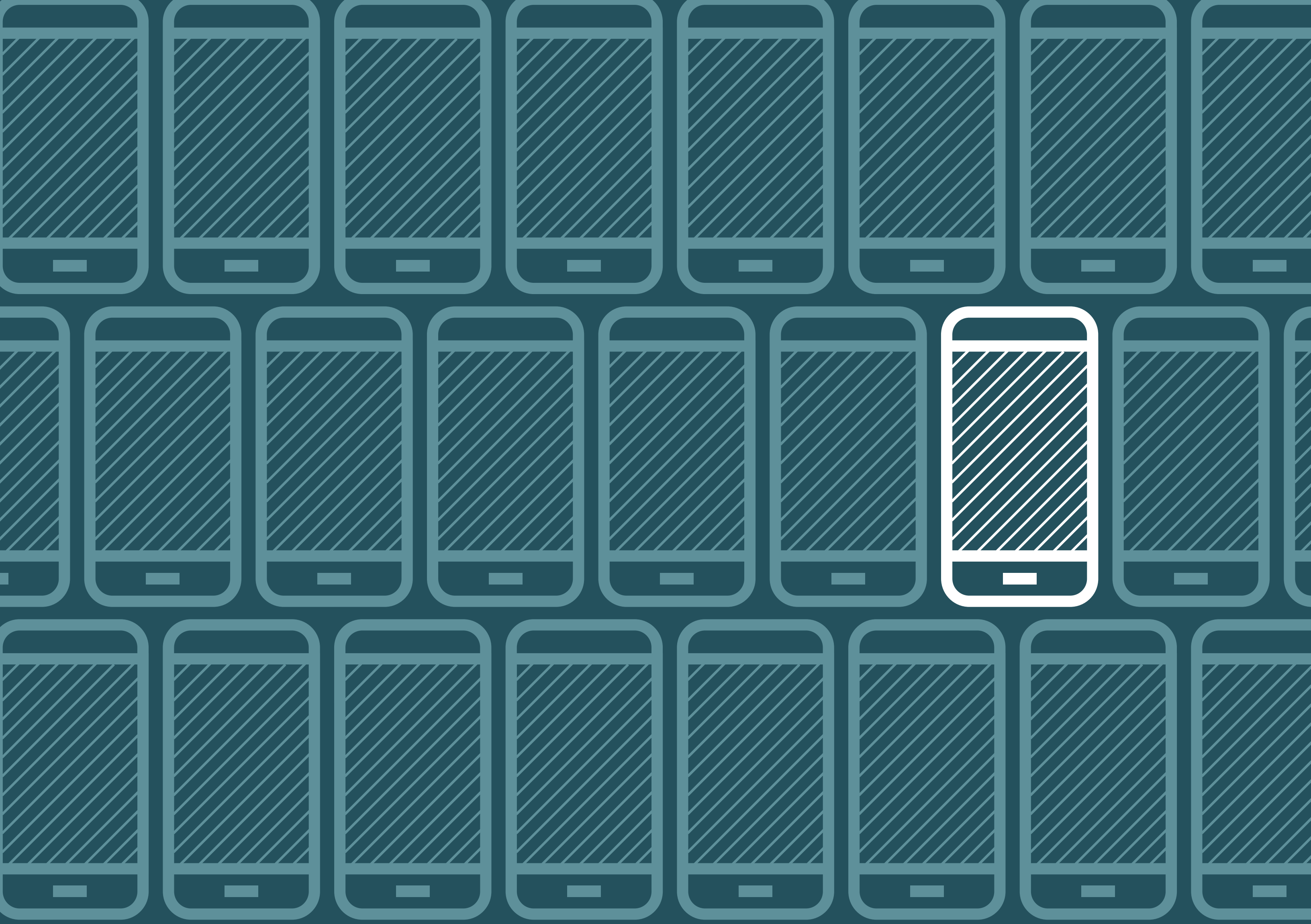
15.8 REASSIGNED NUMBERS DATABASE

Once operational, calling parties will be able to utilize a centralized, comprehensive Reassigned Numbers Database (RND) to avoid calling numbers that have been reassigned. Specifically, based on data reported by carriers to the RND Administrator, a caller will be able to search the RND for a number and a date to determine whether the number has been disconnected since the date in question.[76] Thus, callers will be able to make calls, including robocalls, only to those individuals from whom they have the requisite level of consent. The process to procure an RND Administrator is underway.

[74] Google, "Phone App Help: Screen Your Calls Before You Answer Them," https://support.google.com/phoneapp/answer/9118387?hl=en.

[75] Phone by Google - Caller ID & Spam Protection, Phone Application, https://play.google.com/store/apps/details?id=com.google.android.dialer

[76] Advanced Methods to Target and Eliminate Unlawful Robocalls, CG Docket No. 17-59, Second Report and Order, 33 FCC Rcd 12024, (released Dec. 13, 2018), para. 19. Toll-free numbers also will be included in the database. Id. at 12033, paras. 22-23.



16

DISPLAY TO CALLED PARTY

DISPLAY TO CALLED PARTY

The industry led Robocall Strike Force highlighted the need to provide the called party with a greater degree of identification and control over the calls they receive. The Strike Force recommended the industry deliver a framework for delivering information from the network (including the results of STIR/SHAKEN) to the called party's device. The goal is to empower consumers to make informed decisions and have access to an expanded set of call handling options.

In 2018, the IP-NNI Task Force delivered a framework for the display of verified Caller-ID in ATIS-1000081, ATIS Technical Report on a Framework for Display of Verified Caller ID.[77] The document provides recommendations on "better" display content, backed by usability and comprehension studies. However, the document recognizes that local policy may override the recommendations.

16.1 HUMAN FACTORS

One of the challenging issues in the robocall battle is what should be displayed to the called party after the available network and call information has been analyzed. Should it be a score? Should it be text or a warning sign?

The International Organization for Standardization (ISO) has defined an international language of graphical symbols that provide people worldwide with a coherent set of graphical symbols to help overcome language barriers. However, despite such standards, individual interpretations may still vary.

16.1.1 Hiya Study

Hiya conducted several usability studies in 2018, focusing on the display guidelines for the STIR/SHAKEN protocol. The goals were to:

- Measure the potential impact of a positive indication to the called party (such as a "green checkmark") of verified calls.
- Assess the effectiveness of using text and icons as caution indicators on suspicious calls.
- Hiya conducted three studies on different audiences:
- A user comprehension and influence study on robust caller profiles and certified call markers.
- A user impact analysis of various phrasings and iconography for suspicious call messaging.
- A call pickup rate impact analysis of a "certified" checkmark icon.

The details of each study are published in ATIS-1000081, ATIS Technical Report on a Framework for Display of Verified Caller ID. Table 16.1 summarizes the findings.

Study	Description (Questions for Subjects to Answer)	Results
User comprehension	What do you notice about the screen?	Strong indication that additional caller information strengthens user confidence in the legitimacy of call.
	What confidence do you have in this caller information?	
	What effect does this have on your opinion of previous screens (if any)?	
User impact of phrases and icons, e.g.: "fake number" "possible fraud" "spoofed number" Plus more...	Would you answer this call?	Further studies are needed. However, study showed that less aggressive messages had lower block rates. "Possible Fraud" had the highest block rate, followed by "Spoofed Number" and "Fake Number" (showed that users had a general understanding of the term "spoof").
	Would you block this number from calling in the future?	
Call pickup rate	Calls were created and called party pickup rates were monitored for two weeks.	Further studies are needed.

Table 16.2: Pros and Cons of Reusing the CNAM display field

[77] ATIS-1000081, ATIS Technical Report on a Framework for Display of Verified Caller ID, May 2018, https://www.atis.org/resources/technical-report-on-a-framework-for-display-of-verified-caller-id-atis-1000081/.

ATIS-1000081, ATIS Technical Report on a Framework for Display of Verified Caller ID, recommended that only warning symbols be provided when warranted. Use of multiple symbols may lead to consumer confusion.

16.1.2 TNS Study

TNS[78] conducted a separate user study with 1,000 participants almost equally distributed in demographics: age, gender, income, and education level. Fifty percent were Android users, and the other 50% were iOS users.

The participants were served by the major mobile carriers: 31% from Verizon; 26% from AT&T; 16% from T-Mobile; 9% from Sprint; 1% from US Cellular, and 17% from other carriers. Most participants (80%) had a monthly plan, while 16% were pre-paid.

Thirty-nine percent of participants had no experience with these types of call protection services. Participants were shown different text and icons to compare the effect on call answer rates. The study tested basic (free) and premium (paid) services. The paid services provided an enhanced caller ID display with additional information about the call (beyond name and number).

According to TNS, 80% participants did not answer a call from an unknown number, even when labeled with “TN Validation Passed.” The message did not alter the reaction or significantly increase the answer rate. The study notes that 4 out of 5 calls receiving the basic service are likely to go unanswered. In contrast, with the premium service where enhanced call information is provided, the call answers more than doubles. Fifty-three percent of calls are likely to be answered when the “name” information is provided. With enhanced caller ID (including the name, more information about the caller such as purpose of the call) the answer rate increased to 71% versus 21% answer rate without enhanced caller ID.

In summary, the TNS study concludes that consumers were looking for a restoration of trust in their caller ID services. Delivery of more caller information had greater effect on their decisions to answer than messages or symbols labelling the call “validated/verified.” The results of the TNS study confirmed some of the recommendations in ATIS-1000081, ATIS Technical Report on a Framework for Display of Verified Caller ID.

16.2 SUMMARY OF DISPLAY GUIDELINES FROM ATIS-1000081, ATIS TECHNICAL REPORT ON A FRAMEWORK FOR DISPLAY OF VERIFIED CALLER ID

ATIS-1000081, ATIS Technical Report on a Framework for Display of Verified Caller ID, provides the following display recommendations:

1. When validation fails, use “Fake Number” to alert the called party not to trust the number being presented. If an icon can be presented, the use of a “stop sign” or warning triangle further increases user caution, with negligible impact on block rates. Such a string is short enough to fit in CNAM fields.
2. eCNAM delivers the aggregate of all the information available about the TN (caller identity, results of Call Validation Treatment (CVT) analytics, and information queried by the terminating provider).
3. The use of multiple symbols in a given display is not recommended because the consumer’s interpretation of different symbols may result in confusion and detract from the service’s value.
4. Displaying status symbols such as checkmarks on calls with “full attestation – verification passed” is not recommended. Studies show it confuses consumers.
5. Warning symbols should be provided only when warranted.
6. Give consumers the option of having audible special ringing/tones applied on calls that fail verification.

The recommendations are offered as best practices to SPs, user equipment manufacturers, and analytics services. ATIS-1000081, ATIS Technical Report on a Framework for Display of Verified Caller ID, recognizes variations will exist subject to each SP’s local policy.

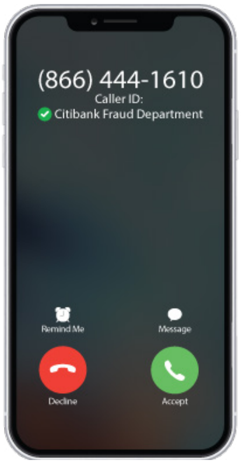
[78] www.tnsi.com. TNS is a supplier of networking and integrated data services to many organizations, as well as a provider of telecommunications network solutions to SPs.

16.3 DISPLAY EXAMPLES AND OPEN ISSUES

16.3.1Use of the Green Check Mark

It has been argued that the use of the green check (Figure 16.1) may pose a risk to the consumer if the calling party number passes verification even though the caller's intentions may be predatory. The FCC has made it clear that its STIR/SHAKEN mandate does not include requiring SPs to display green checks on verified calls. Instead, SPs are free to follow their own local policies about what to display to the called party.

Furthermore, one could argue that overusing the green check icon could dilute its value, and that consumers could become desensitized to the icon's meaning. Cases where a green check accompanies a fraud alert from the consumer's bank could be meaningful to that person — even more meaningful than on a call from a family member. Hence the recommendation to use the green check sparingly.

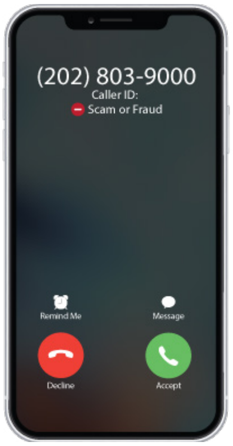


(866) 444-1610
Caller ID:
✓ Citibank Fraud Department

Figure 16.1: Display Example 1

16.3.2 Use of Warning Icons

Conversely, using warning icons and expanded text to warn a consumer against a fraud attempt is what ATIS-1000081, ATIS Technical Report on a Framework for Display of Verified Caller ID recommends. The enhanced CNAM (eCNAM) envelope can deliver additional text and symbols that are easy to understand. Figure 16.2 is an example showing a high-risk assessment from CVT. If, for example, the call is determined to be from a recent known scam, the phrase "Do not give personal info" could be selected and delivered to the consumer. Including a red circle or octagon helps draw the called party's attention.



(202) 803-9000
Caller ID:
⛔ Scam or Fraud

Figure 16.2: Display Example 2

16.3.3 SP Local Policy

For the foreseeable future, it is expected that each SP and its analytics service will select the format and content of the display for their customers without universal standards. Given that the interface to the UE is standardized, the content, as a payload, could vary without changes to the interface. This flexibility allows SPs and CVTs to adjust their display for new scams.

16.4 DATA INTEGRITY AND CHOICES OF DATA SOURCES FOR CALLING NAME

The deployment of SS7 in the mid-1980s created the ability to pass calling information (primarily the Calling Party Number (CPN)), as well as utilizing query and response signaling. With the ability to query other network elements, SPs were able to offer services such as CNAM where the user information was maintained in most SPs' databases.

If a SP chose not to have its own database, it could store its records in some other authoritative database, regardless of the database's geographic location. The SP would function in the same way as the database owner regarding the maintenance of data accuracy.

Resellers of TNs are considered customers of the SP that sold them the TN. Consequently, the TNs assigned to the reseller are stored in the same authoritative database.

CNAM is a terminating subscription service, so the service logic resides in the terminating network serving the subscriber. Once the calling party number is received, the terminating network verifies the user is a valid CNAM subscriber. If the subscription is valid, the following steps are carried out by the TSP:

1. If the received calling number is anonymous (aka private), then a CNAM query will NOT be launched.[79]
2. If the calling number is not anonymous, a query is launched to the appropriate database. (Database addresses are discovered through global title translations from routing tables such as the CNAM Routing Guide (CNARG)).
3. The result of the query is returned to the network that sent the query to display to the subscriber a name or, if no name was found, an indication of "unavailable."

Major SPs obtain the data from the source (i.e., customer service orders). Major SPs are meticulous about maintaining these databases, emphasizing accuracy and data integrity. Data is updated in near real time to reflect service changes (e.g., disconnects, account changes). As a result, when the TSP queried one of these authoritative databases, the quality of the CNAM service nationwide remained very high through the '80s, '90s, and early 2000s. The CNARG is the source used to administer and maintain routing to these authoritative databases (via Global Title Translations tables). According to the standards, these databases are designed with a maximum downtime of 12 hours annually. However, there have been no reported outages since their deployment.

But in the early 2000s, interconnection agreements to query those databases receded. New, non-authoritative data sources emerged with lower data integrity standards. Typically, the data was obtained from third parties and the information was outdated. SPs that decided to query those non-authoritative sources delivered wrong or outdated names to their end-users.

Furthermore, some of these data sources operated unethically. They collaborated with fraudsters to store false data in association with the TNs used by fraudsters (e.g., Bank of America or the IRS against TNs not assigned to Bank of America or the IRS) to help the fraudsters facilitate their scams. By contrast, major SPs have always followed strict vetting and verification steps before storing names in their databases, even though there never was any regulatory or industry requirement to do so.

During the early stages of wireless offerings to the public, SPs relinquished the display of a name to the handset-based contacts list. At the time, most wireless customers only shared their TNs with a limited list of friends and family members due to costly, limited-minutes plans. To conserve minutes, wireless customers were reluctant to answer incoming calls from callers outside their contact list. As a result, wireless SPs did not see any advantage for following the CNAM model of querying a name database and delivering the name to its end users.

Today, virtually all wireless providers store their lines in an authoritative database of their choosing. That way, when a wireless customer calls a TDM number, the terminating office can launch a query and retrieve the wireless subscriber's CNAM. However, virtually no wireless SP has chosen to provide the CNAM when a call terminates with them. This is a business decision that the wireless SPs made a long time ago and may need to revisit.

Today, more than 50% of subscribers are wireless-only users, and the prior concern over per-minute charging is no longer valid due to the prevalence of unlimited plans. Those subscribers should have access to the call management benefits of services such as CNAM delivery service that they once had with wireline service, especially now that callers (in their contact list or not) can reach them only on their wireless phones.

Even prior to the industry's battle with robocalling, it was evident that the quality of CNAM was dropping. As a symptom of robocall fraud, spoofing undermines virtually all services relying on the delivered calling number. The impact is not unique to CNAM. As STIR/SHAKEN implementation reduces spoofing, CNAM regains its high-quality state. However, as discussed above, the larger issue remains that the industry has relinquished best practices and guidelines that served consumers and enterprises well for two decades.

Exposure to robocalling and its damage to call management services shed light on the needs and expectations that consumers and businesses developed over the years. Consumers continue to expect a higher level of accuracy from the next generation of these services to empower them to make decisions based on that service display. Although STIR/SHAKEN repairs one defect in the overall fabric, the fundamental accuracy issue still needs to be addressed.

The following are considerations for improving the quality of the display.

- Enhanced Identity and Name Database Providers must verify that the holder of a TN is authorized to use the display name, company logo, and other information delivered to called users for calls originating from that TN.
- SPs should be accountable for decisions to retrieve CNAM and metadata from non-authoritative sources.
- Wireless SPs are strongly encouraged to offer a comparable identity service delivery, such as enhanced CNAM, to their customers.
- Secure the IP interfaces between the query originator and the authoritative databases to avoid potential data corruption.

[79] FCC Docket 91-281 ordered that name presentation must follow number presentation (i.e., if the calling number is anonymous, the calling name displayed to the called party will be "anonymous" as well).

Finally, it should be noted that almost all the authoritative databases support protocol conversion to facilitate almost any IP-based protocol if the query originator does not support SS7 messaging.

16.5 ENHANCED CNAM (eCNAM)

While CNAM is an SS7-based service, eCNAM is a terminating IP Multimedia Services (IMS) feature that will likely reside in the carrier's Telephony Application Server (TAS). More importantly, eCNAM provides a name longer than the CNAM's 15-character limit. eCNAM also offers metadata about the caller beyond the name.

Upon receiving a terminating INVITE request, the TSP queries an authoritative database, using the calling TN as the key, to obtain calling display name and other metadata. To ensure that the data is accurate, the TSP must ensure that the calling TN correctly identifies the originating customer (e.g., by using a calling TN received in a valid PASSporT).

The eCNAM specifications stress the critical importance of retrieving data from authoritative databases to maintain the service's integrity. Authoritative databases employ vetting procedures early in the data storage and account setup phase that ensure the data provided by the TN holder reflects the correct information identifying them (e.g., name, business name, type of business, logo, location such as city and state). Retrieving and delivering inaccurate data to consumers could increase their confusion and enable exploitation by bad actors.

Based on the provider's local policy, robocall analytics services could relay their call assessment results to the TAS. The universe of messages that analytics services are expected to produce is mostly in the form of readable text and icons. The name is delivered in the display-name parameter of the From header field or the PAI header field to the User Endpoint (UE). The metadata and robocall-related data (including logos or icons) are to be delivered in one or more Call-Info headers. The Call-Info headers are expected to be populated by the terminating TAS and sent directly to the UE. These Call-Info headers are not from the originating or intermediate networks. Instead, they are created by the terminating network to securely transmit all the metadata and analytics over the final interface to the UE.

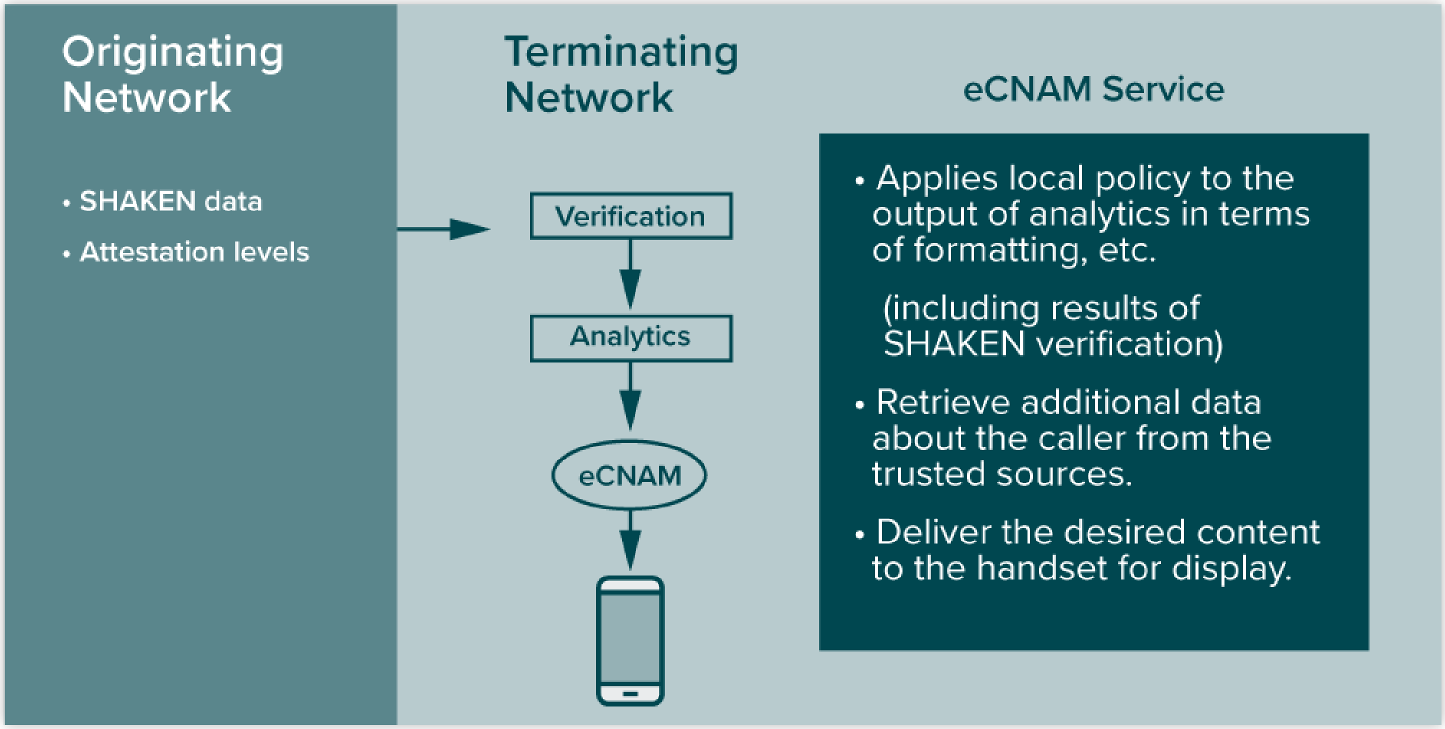

Originating Network
• SHAKEN data
• Attestation levels
Terminating Network
Verification
Analytics
eCNAM
eCNAM Service
• Applies local policy to the output of analytics in terms of formatting, etc.
(including results of SHAKEN verification)
• Retrieve additional data about the caller from the trusted sources.
• Deliver the desired content to the handset for display.

Figure 16.3: eCNAM

eCNAM is described in:

- ATIS-1000067.2015[80]
- 3GPP TS 22.173, IMS Multimedia Telephony Service and supplementary services; Stage 1 (Release 15) in 2016[81]
- 3GPP TS 24.196, Enhanced Calling Name (eCNAM); (Release 15) in 2018[82]

[80] ATIS-1000067.2015(R2020), IP NGN Enhanced Calling Name (eCNAM), August 1, 2015, https://www.techstreet.com/standards/atis-1000067-2015-r2020?product_id=1900475

[81] 3GPP TS 22.173, IMS Multimedia Telephony Service and Supplementary Services; Stage 1, Release 15, 2016, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=620.

[82] 3GPP TS 24.196, Enhanced Calling Name (eCNAM), Release 15, 2018, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3238.

16.6 ADVANTAGES OF eCNAM

- eCNAM's flexible "delivery mechanism" supports delivery of text strings and icons/symbols in an "envelope" as a payload to be rendered on any screen, independent of the content.
- This frees each carrier to deliver its own unique combination of text and icons to its subscribers without requiring changes to existing standards.
- As a terminating service, eCNAM gives TSPs control over the data being displayed and delivers the benefits of analytics to the end user.
- eCNAM is a single service that integrates (for the SP) the elements of the final display from various sources of data and call verification functions.

16.7 eCNAM AND ALTERNATIVE IDENTITY DELIVERY METHODS

A current draft specification under the ATIS IP-NNI Task Force introduces a PASSporT extension for enhanced calling data, such as logos and other extensible information and is referred to as "Rich Call Data (RCD)" or "rcd", as described in Section 17.

For both the eCNAM and RCD mechanisms, it is important that the enhanced calling data is vetted by a trusted entity to prevent misinformation from being relayed to the called party. In the case of authoritative databases used by eCNAM, the trusted entity is the eCNAM database provider working directly with its customers as their TNSP. The Authoritative Databases' Owner (ADO) has followed self-imposed practices on data vetting of the records stored in their databases. The databases host almost all working TNs. For the majority of these records, the ADO is also the TNSP and CSP. Some of the records are of TNs served by other carriers (such as resellers and wireless SPs that do not operate a database of their own), which are referred to as storage customers or tenants.

The contracts between the ADO and those tenants contain terms for penalties or termination from the authoritative database if the tenant deliberately misrepresents any information associated with its TNs. The purpose is to ensure no one is using the database to deliver misleading information. Maintenance and audits are part of the daily operation. Historically, storage customers were terminated when audits and fraud systems revealed any attempts to defraud the ADO or others.

In the case of an "rcd" PASSporT, the trusted entity is anticipated to be a vetting agency authorized by the STI-PA to perform a similar role in verifying the data included in the "rcd".

The TSP local policy determines the content displayed to the called party. The TSP can receive validity information via the SHAKEN PASSporT or by other unspecified means. If the OSP cannot verify the "rcd" information, and the TSP cannot trust such content, it should not propagate it to its end users.

Furthermore, eCNAM is not only a call management service that delivers metadata. It also provides a means to compile and deliver the final display, including the results of analytics, to the called UE. Therefore, if "rcd" and eCNAM are both available and trusted by the TSP, these are the possible outcomes or interactions in terms of a) how the TSP compiles the display information to be delivered to the called party and b) how the display information is carried in the INVITE request sent to the called UE. Figure 16.4 illustrates the process:

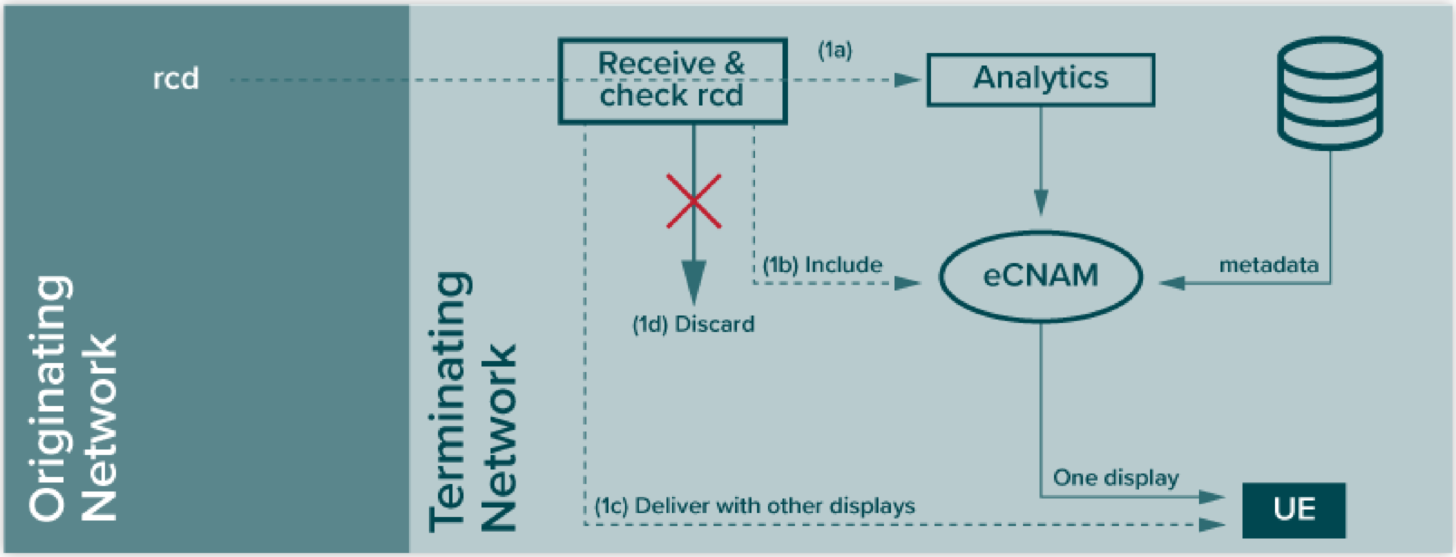


Figure 16.4: eCNAM and rcd Interactions

- 1a: RCD content is directed to and is consumed by analytics. eCNAM delivers metadata, and the results of analytics in the From, PAI, and Call-Info header fields in the INVITE request are sent to the called UE.
- 1b: The TSP trusts the rich call data information received in a SHAKEN PASSporT and decides to include some or all of this information in the eCNAM envelope, in addition to eCNAM metadata, in the From, PAI, and Call-Info header fields of the INVITE request sent to the called UE.
- 1c: The TSP trusts the rich call data information received in a SHAKEN PASSporT, which it delivers in the INVITE request sent to the called UE separately from the eCNAM call information (to be displayed together without combining their respective content).
- 1d: The TSP also has the option of discarding the rich call data information received in a PASSporT for a variety of reasons.

In STIR/SHAKEN's early deployment stages, or in the absence of RCD (for any reason), eCNAM and the appropriate input from analytics services together can provide end users with a display that informs, protects, and empowers them to manage their calls. The eCNAM core capabilities of retrieving the name and metadata already exist within most networks.

The flexibility of expanding the content in eCNAM Call-Info header fields will support the delivery of future content such as logos and pictures. If the logo or picture is to be retrieved via a URL, the TSP may provide the address at a trusted database in the eCNAM display for the UE to launch.

16.8 LEGACY CONSUMER SOLUTIONS

SIP-based STIR/SHAKEN mechanisms are intended for users of IP networks. The industry recognized at an early stage that most of the verification efforts will not be available to legacy users. This segment of the population is typically targeted by fraudsters. The FCC has asked the industry to develop anti-robocalling solutions for the TDM population, despite the technology limitations.

Given the significant amount of TDM infrastructure currently in place and the significant impact to this infrastructure that changes would present, these solutions are expected to be created with minimal to no changes to the existing TDM infrastructure (e.g., SS7 signaling, the interface between the network and the caller ID devices, end office equipment). Taking all the variables into account, the industry introduced an option where some of the benefits of analytics services may be relayed to TDM customers on their analog displays. This could be viewed as a case of "re-use" of existing devices and interfaces.

The guidelines suggested a single character (such as an asterisk) to prepend or append the name being displayed to alert end users about the call status (good call or scam). That idea's pros and cons were documented, citing possible abuse by scammers. Prepending a character, such as an asterisk that indicates a call is verified, could be easily mimicked by bad actors. Callers with intent to defraud would easily insert or spoof that character in the caller ID information to trick the customers trained to trust calls with that prepended character.

Following the publication of ATIS-1000081, the implementation in some carrier networks did not use the asterisk. Instead, a display that clearly includes the text "Scam?" or "Spam?" for suspicious calls was implemented. However, some carriers continue to use a single character (e.g., [v]). While there are no standard service descriptions of this work-around, a generic example is provided and the modified CNAM service could potentially operate as follows:

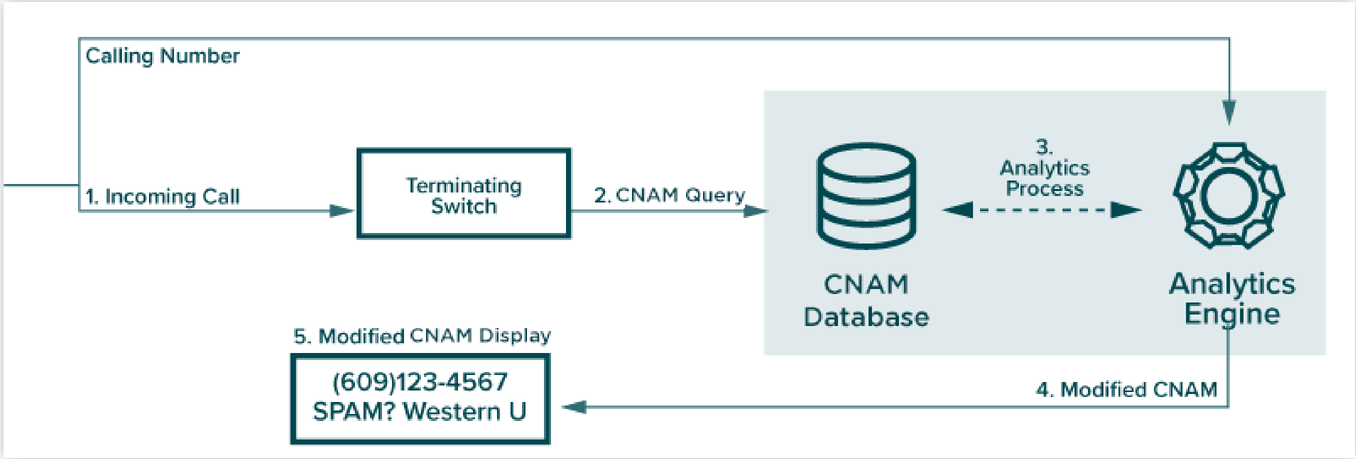


Figure 16.5: Potential Implementation of Modified CNAM Display

1. An incoming call triggers a CNAM query to the appropriate database.
2. The analytics service employed by the SP would simultaneously assess the risk of the call. Note that each analytics service has different criteria and thresholds on what will be reported/displayed to the user as a "suspicious" call.
3. If a call is deemed "suspicious," the returned name string (from the Name database) needs to be modified. A new function will be needed to pre-pend the warning text "Scam?" or "Spam?" and include the first nine characters of the name received from the database.
4. The modified CNAM string is modified before it is returned to the terminating switch.
5. The warning text alerts TDM customers with analog devices of potentially fraudulent callers, thus extending the benefits of analytics to this population.

Given the lack of any standard solution for the legacy consumers, the above workaround appears to be an improvement. However, like any other proposal, there are pros and cons, as Table 16.2 summarizes.

Pros	Cons
Extend the benefits of analytics to TDM, which tends to encompass some of the more vulnerable demographics.	The warning may not distinguish between fraudulent robocalls and legitimate robocalls such as charities or businesses with a legitimate relationship to the consumer.
Satisfy some FCC expectations.	The costs of the modifications may not be recoverable if the SP is expected to provide it to consumers without charge.
Re-use and build on existing CNAM functions.	The warning text consumes significant space in an already limited 15-character display.
Consumers understand the message "scam?" without the need for extensive education.	The nine characters used for the name string may not be sufficient to convey the name of the calling party and could result in consumer complaints.
Consumers keep their existing caller ID equipment.	There may be royalties associated with this solution.

Table 16.2: Pros and Cons of Reusing the CNAM display field

17

FRAMEWORK FOR CONVEYING VETTED RICH CALL DATA VIA "RCD" PASSPORT

The forthcoming ATIS standard for Calling Name and Rich Call Data Handling Procedures is expected to extend the base SHAKEN framework defined in ATIS-1000074 to enable rich call data authorized for a calling user to be conveyed in a SHAKEN or “rcd” PASSporT from the originating network to the terminating network. Conveying rich call data in a PASSporT signed by an originating network provides a number of benefits. For example, it gives an originating enterprise customer more control over the form and content of the rich call data that the called party sees. Also, the integrity protection provided by conveying the information in a signed “rcd” PASSporT enables verifiers to detect when an unauthorized entity modifies the rich call data (e.g., when a malicious entity modifies the contents of a pass-by-reference file containing a company logo). Furthermore, this mechanism avoids an issue associated with traditional terminating CNAM services, where TSPs are incented to obtain calling name information from low-cost CNAM data sources that do not necessarily provide up-to-date and vetted information (see Section 16.4).

The mechanisms described in the forthcoming ATIS standard for Calling Name and Rich Call Data Handling Procedures are based on “draft-ietf-stir-passport-rcd,” which defines a new “rcd” PASSporT type containing three new claims:

- An “rcd” claim that contains a display name component, and either a jCard component or an HTTPS URL reference to a remote jCard resource. (jCard is an extensible JSON object that carries rich information about the calling entity such as company logo.)
- A crn claim that contains a call reason phrase.
- An rcdi claim that contains a digest of the rich call data information conveyed by the rcd claim, including referenced information. The rcdi claim enables verifiers to detect if an unauthorized entity has modified the referenced rich call data.

To ensure the accuracy of the information conveyed in an “rcd” PASSporT, a vetting service provided by the TNSP or a third-party vetting agency authorized by the STI-PA verifies the calling customer’s authority to use the rich call data. The vetting agency is identified in the signing delegate certificate chain of the “rcd” PASSporT so that it can be easily identified during traceback activity.

Figure 17.1 shows how “rcd” PASSporT extends the base SHAKEN framework to support rich call data. The diagram shows the base SHAKEN authentication/verification procedure. A SHAKEN Identity header added by an Originating Network STI-AS is carried in the INVITE request to the Terminating Network and verified by the STI-VS. To support rich call data, an RCD Authentication Service (RCD-AS) in the Originating Network constructs an “rcd” PASSporT containing rich call data information authorized for the calling user. The “rcd” PASSporT is conveyed in a second Identity header field in the INVITE request to the Terminating Network. An RCD Verification Service (RCD-VS) in the Terminating Network verifies the received “rcd” PASSporT and renders the validated rich call data to the called party.

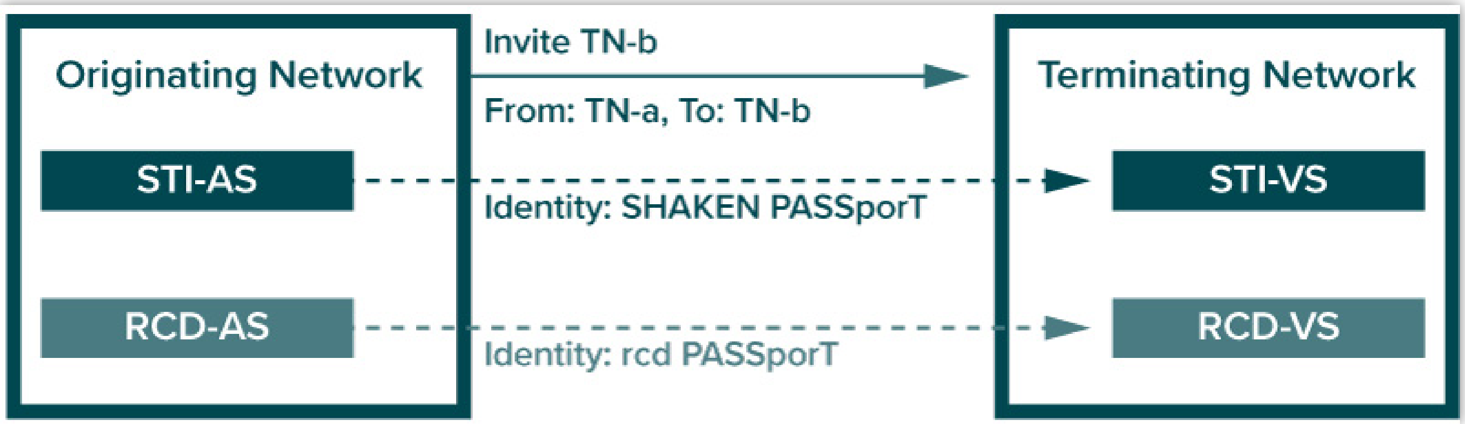


Figure 17.1: Delivering rich call data via “rcd” PASSporT

18 REGULATORY

18.1 FEDERAL ACTIVITY

Stopping illegal and unwanted robocalls has been one of the FCC's top consumer protection priorities for several years. In July 2016, then-FCC Chairman Tom Wheeler issued a call to action to the industry to take additional steps to stop robocalls.[83] This ultimately led to the industry led Robocall Strike Force, which developed recommendations for implementing STIR/SHAKEN, call blocking solutions, traceback, and regulations, among other issues.[84] The FCC followed with guidance regarding call blocking and then, under Chairman Ajit Pai, a number of additional robocall blocking and call authentication proceedings.

The TRACED Act was enacted into law on December 30, 2019, to enhance the efforts of the FCC and industry. The law requires the FCC to undertake a significant number of reports and rulemakings on issues ranging from:

- Timelines for implementation of call authentication.
- Ways to enhance enforcement for legal/regulatory violations.
- Industry traceback efforts.
- Ways to address one-ring scams.

The FCC's implementation of the TRACED Act is well underway.

18.1.1 Call Authentication Frameworks

The TRACED Act requires that voice SPs implement call authentication processes to ensure caller ID information is appropriately authenticated. To ensure timely adoption, the law requires the FCC to mandate STIR/SHAKEN for voice providers in IP networks. It also requires reasonable measures to implement call authentication in non-IP voice networks within 12 months of enactment (by December 30, 2020), subject to certain extensions as the agency believes appropriate.

In March 2020, the FCC issued an order mandating that voice SPs implement the STIR/SHAKEN caller ID framework in the IP portions of their network by June 30, 2021—to the extent such providers have not already voluntarily implemented the framework—and seeking comment on a number of implementation issues.[85] In September 2020, the FCC issued another order, adopting certain extensions to the STIR/SHAKEN mandate, including for small voice SPs and for non-IP networks. This order requires voice SPs to (1) completely upgrade their non-IP networks to IP and implement STIR/SHAKEN on their entire network or (2) work to develop a non-IP authentication solution, either on their own or through a third-party representative, such as a trade association by participating as a member of a working group, industry standards group, or consortium.[86]

The FCC's September order also adopted a new certification requirement related to robocall mitigation. Under the FCC's approach, once effective, providers will need to certify that they have implemented STIR/SHAKEN for the calls they originate or otherwise certify that they have implemented an appropriate robocall mitigation program. The appropriate robocall mitigation program requirement generally is not prescriptive. One exception is that all providers must commit that they will respond fully and in a timely manner to all traceback requests from the FCC, law enforcement, and the industry traceback consortium. They also must cooperate with such entities in investigating and stopping any illegal robocallers that use their services to originate calls. Providers' certifications will be included in a new FCC Robocall Mitigation Database. Intermediate providers and voice SPs will be permitted only to accept calls directly from a voice SP, including a foreign voice SP that uses NANP resources that pertain to the U.S. to send traffic to residential or business subscribers in the U.S., if that provider's filing appears in the Robocall Mitigation Database.

The TRACED Act also requires the FCC to assess call authentication deployment and efficacy and to submit a report to Congress not later than December 30, 2020. This report will assess:

- The extent to which providers of voice service have implemented the call authentication frameworks, including whether the availability of necessary equipment and equipment upgrades has impacted such implementation.
- The efficacy of the call authentication frameworks in addressing all aspects of call authentication.
- By December 30, 2020, the FCC must issue best practices that voice SPs may use as part of the implementation of effective call authentication frameworks to ensure that the calling party is accurately identified.

[83] Tom Wheeler, "Cutting off Robocalls," FCC Blog, July 22, 2016, https://www.fcc.gov/news-events/blog/2016/07/22/cutting-robocalls.

[84] See Robocall Strike Force Report, Oct. 26, 2016, https://www.fcc.gov/sites/default/files/robocall-strike-force-final-report.pdf.

[85] Call Authentication Trust Anchor, WC Docket Nos. 17-97 and 20-67, Report and Order and Further Notice of Proposed Rulemaking, 35 FCC Rcd 3241, 3243 (2020), https://docs.fcc.gov/public/attachments/FCC-20-42A1.pdf, para. 3.

[86] Call Authentication Trust Anchor, FCC 20-136, WC Docket No. 17-97, Second Report and Order (2020) https://docs.fcc.gov/public/attachments/FCC-20-136A1.pdf, para. 24.

18.1.1.1 Review and Revision/Replacement

No later than three years after enactment (December 30, 2023), and every three years thereafter, the FCC must analyze and issue a report on the efficacy of the technologies used for call authentication frameworks. The FCC must also determine whether the required call authentication framework needs to be revised or replaced. Then, it must compile this information along with any proposed actions and submit this report to Congress.

18.1.1.2 Service Provider Access to the SHAKEN Ecosystem

One gating factor for full implementation of STIR/SHAKEN per the TRACED Act and FCC rules is the "SPC token Access Policy." Participation in the U.S. SHAKEN ecosystem allows an SP to acquire the credentials to authenticate itself as an OSP and to protect the integrity of the calling TN information. It is controlled by this policy set by the STI-GA (Secure Telephone Identity – Governance Authority). SHAKEN SPs are required to file an FCC 499-A universal service contributor form and have a standard telecom company identification code (Operating Company Number (OCN)).

The initial STI-GA requirements for SPs issued in August 2019 also included a provision that any SHAKEN SP is required to have "direct access to telephone numbers" from the North American numbering administrators. Several commenters to FCC proceedings and to the STI-GA Board noted that this last requirement limits SHAKEN SP credential access mostly to traditional telecom carriers and certain entities classified as "Interconnected VoIP SPs" that are authorized to access TN resources. However, the set of entities required to implement STIR/SHAKEN under the TRACED Act and accompanying FCC rules is more broadly defined.

In November 2020, the STI-GA revised the policy to remove the requirement for direct access to TN resources. This requirement was replaced with a requirement that entities "[h]ave certified with the FCC that they have implemented STIR/SHAKEN or comply with the Robocall Mitigation Program requirements and are listed in the FCC database," with the new policy effective date coinciding with the filing deadline for entities to certify their robocall mitigation programs. As the filing deadline is subject to further FCC implementation and will be "no earlier than June 30, 2021," per FCC rules, the current more restrictive policy will be in effect until then. The rules promulgated in the FCC's Second Report and Order account for this fact. They offer an extension under certain conditions to entities that are pursuing SP Code (SPC) token Access under the current policy or that may be able to qualify under the (then anticipated) future policy.

18.1.2 Call Blocking

The FCC issued a number of orders authorizing voice SPs to block illegal and unwanted robocalls. Specifically, the FCC clarified that voice SPs may block calls from phone numbers on a Do-Not-Originate (DNO) list and those that purport to be from invalid, unallocated, or unused numbers. SPs may block these calls on an opt-out basis where reasonable analytics indicate the calls are unwanted and, on an opt-in-basis, from numbers that are not on a customer's whitelist.[87]

In addition, the FCC has adopted two safe harbors for voice SPs that inadvertently block wanted calls as part of their call blocking programs. Consistent with the requirements of the TRACED Act, the FCC's first safe harbor protects terminating voice SPs from liability under the Communications Act and FCC rules if they block calls based on reasonable analytics, as long as they take into account call authentication information when available for a particular call.

The second safe harbor authorizes voice SPs to block traffic from "bad actor" upstream voice SPs that continue to allow unwanted calls to traverse their networks. Specifically, a provider may block voice calls or cease to accept traffic from an originating or intermediate provider that, when notified by the FCC, fails to effectively mitigate illegal traffic within 48 hours or fails to implement effective measures to prevent new and renewing customers from using its network to originate calls. Prior to initiating blocking, the provider must give the FCC notice and a brief summary of the basis for its determination that the originating or intermediate provider meets one or more of the conditions.

In addition, as required by the TRACED Act, the FCC adopted certain protections against erroneous blocking. First, the FCC required that voice SPs make "all reasonable efforts" to ensure that calls from PSAPs and government outbound emergency numbers are not blocked. Second, the FCC required that any voice SP that blocks calls designate a single point of contact for callers, as well as other voice SPs, to report blocking errors at no charge to callers or other voice SPs. Blocking providers must investigate and resolve blocking disputes in a reasonable amount of time and at no cost to the caller, as long as the complaint is made in good faith.[88]

[87] Advanced Methods to Target and Eliminate Unlawful Robocalls, CG Docket No. 17-59, Report and Order and Further Notice of Proposed Rulemaking, 32 FCC Rcd 9706, (2017), https://docs.fcc.gov/public/attachments/FCC-17-151A1.pdf, para. 1.
Advanced Methods to Target and Eliminate Unlawful Robocalls, CG Docket No. 17-59 and WC Docket No. 17-97, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, 34 FCC Rcd 4876, 4877, (2019), https://docs.fcc.gov/public/attachments/FCC-19-51A1.pdf, para. 2.

[88] Advanced Methods to Target and Eliminate Unlawful Robocalls, CG Docket No. 17-59, Third Report and Order, Order on Reconsideration, and Fourth Further Notice of Proposed Rulemaking, 35 FCC Rcd 7614, 7634, (2020), https://docs.fcc.gov/public/attachments/FCC-20-96A1.pdf, para. 54.

The safe harbors and other associated rules took effect on October 14, 2020.[89] The FCC currently is considering extending the safe harbor for reasonable analytics to network-based blocking.[90]

18.1.3 Enhancing Enforcement

The TRACED Act also enhances the government's enforcement capabilities for violations of the TCPA, which restricts telephone telemarketing and the use of automated telephone equipment. For example, the law establishes civil penalties for TCPA violations, eliminates a requirement that a citation is issued prior to imposition of a civil penalty, and adds an additional penalty of up to $10,000 for intentional violations. The statute of limitations for violations is extended from one to four years.

The law also requires the FCC, in consultation with the FTC, to submit a report to Congress within one year (and annually thereafter) about robocall enforcement, including the number of:

- Complaints received during each of the preceding five calendar years.
- Citations issued by the FCC during the preceding calendar and details of each such citation.
- Notices of apparent liability issued by the FCC, including any proposed forfeiture amount.
- Final orders imposing forfeiture penalties by the FCC during the preceding calendar year, and details of each including the forfeiture imposed.
- The amount of forfeiture penalties or criminal fines collected, during the preceding calendar year, by the FCC or the U.S. Attorney General, and details of each case in which such a forfeiture penalty or criminal fine was collected.
- Proposals for reducing the number of calls made in violation of the TCPA.
- An analysis of the contribution by providers of interconnected VoIP service and non-interconnected VoIP service that discount high-volume, unlawful, short-duration calls to the total number of calls made in violation of such subsections, and recommendations about how to address such contribution in order to decrease the total number of calls made in violation of the TCPA.

In addition, the law requires the Attorney General to convene an interagency task force to study the government prosecution of robocall violations in consultation with the FCC. Among other things, the Working Group will:

- Determine how federal law and budgetary constraints inhibit enforcement of the robocall violations.
- Identify existing and additional policies and programs to increase coordination between federal departments and agencies and the states for enforcing and preventing violations of the robocall violations.
- Identify existing and potential international policies and programs to improve coordination between countries in enforcing robocall violations and similar laws.

The FCC is also charged with providing evidence of willful violations of the TCPA to the Attorney General. The act directs the FCC's Enforcement Bureau Chief to provide any evidence obtained that suggests a "willful, knowing and repeated robocall violation" with an intent to defraud, cause harm or wrongfully obtain anything of value. The FCC must also publish on its website, and submit to Congress within one year, a report that provides the number of instances of the provision of such evidence and a summary of types of robocall violations to which such evidence relates.

Finally, on the issue of enforcement, the FCC is required, no later than 18 months of enactment (by June 30, 2021), to issue regulations establishing a process that streamlines how a private entity may voluntarily share information with the FCC about calls made or text messages sent for which misleading or inaccurate caller ID information was transmitted in violation of the TCPA's prohibition against unlawful spoofed calls.

18.1.4 Traceback

The TRACED Act also addresses efforts to trace the sources of illegal robocalls. It specifically requires the FCC to establish a process by which a single consortium that conducts private-led efforts to traceback the origin of suspected unlawful robocalls can be registered. The act requires that the consortium:

- Be a neutral third party competent to manage such a traceback effort.
- Maintain a set of written best practices about the management of such efforts and providers of voice services participating in such efforts.

[89] See Notice of Effective Date for Call Blocking Rules, CG Docket No. 17-59, Public Notice, (released Sept. 18, 2020), https://docs.fcc.gov/public/attachments/DA-20-1109A1.pdf.

[90] Advanced Methods to Target and Eliminate Unlawful Robocalls, CG Docket No. 17-59, Third Report and Order, Order on Reconsideration, and Fourth Further Notice of Proposed Rulemaking, 35 FCC Rcd 7614, 7616, (2020), https://docs.fcc.gov/public/attachments/FCC-20-96A1.pdf, para. 4.

- Focus on fraudulent, abusive or unlawful traffic.
- File a notice with the FCC that the consortium intends to conduct private-led efforts to trace back in advance of such registration.

In July 2020, the FCC designated the Industry Traceback Group as the single consortium to conduct private-led traceback efforts.[91] The TRACED Act requires the FCC to conduct the process to register the consortium annually.

The FCC currently is considering imposing a broad, affirmative requirement on voice SPs to cooperatively participate in tracebacks.[92] In the meantime, the agency has adopted a traceback requirement for traffic that is not signed under STIR/SHAKEN. This will take effect in June 2021, as well as a requirement for intermediate providers to cooperatively participate in tracebacks if they do not authenticate unauthenticated traffic under STIR/SHAKEN.[93]

The TRACED Act also requires the FCC to make publicly available on its website, and file with Congress within 12 months (by December 30, 2020), and annually thereafter, a report on the status of private-led efforts to traceback the origin of suspected unlawful robocalls.

Under the TRACED Act, the FCC also must issue a study regarding whether to require a provider of covered VoIP service to maintain current contact information on file at the FCC and retain records of each call transmitted over the service that is sufficient to trace such calls back to the source. The FCC must report results to Congress within 18 months of enactment (by June 30, 2021).

18.1.5 Protection from One-Ring Scams

The act also requires the FCC to initiate various measures associated with the one-ring scams. It must initiate a proceeding to protect called parties from such scams, including by considering:

- Incentivizing providers to stop calls made to perpetrate one-ring scams, including whether to allow blocking of numbers involved in these scams.
- Establishing obligations on international gateway providers that are the first point of entry for these calls into the U.S. This includes potentially requiring such providers to verify with foreign originators the nature/ purpose of calls before initiating service.

The FCC issued a Notice of Proposed Rulemaking on one-ring scams in April 2020.[94] Under the TRACED Act, it must publish on its website and submit a report to Congress on the status of one-ring scam proceeding by December 30, 2020.

18.1.6 Numbering Resources

Another focus of the TRACED Act is how to manage numbering resources to mitigate robocall impacts. The law requires the FCC to determine how its policies regarding access to number resources, including number resources for toll-free and non-toll-free TNs, could be modified to help reduce access to numbers by potential perpetrators of illegal robocalls. If the FCC determines modifications could help in this regard, it is required to prescribe regulations to implement the modifications. The FCC sought comment on whether and how it should modify its policies regarding access to toll-free and non-toll-free numbering resources in March 2020.[95] It has not yet taken further action.

18.1.7 Hospital Robocall Protection Group

In recognition of some of the unique risks posed by illegal robocalls to hospitals, the TRACED Act directed the FCC to establish a Hospital Robocall Protection Group (HRPG),[96] which the agency did in March 2020.[97] The HRPG consists of representatives from hospitals, federal and state government agencies, consumer advocates, analytics providers, and voice SPs, and is charged by Congress with issuing best practices regarding:

[91] 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, 35 FCC Rcd 7886, 7886-87, (2020), https://docs.fcc.gov/public/attachments/DA-20-785A1.pdf, para. 3.

[92] Advanced Methods to Target and Eliminate Unlawful Robocalls, CG Docket No. 17-59, Third Report and Order, Order on Reconsideration, and Fourth Further Notice of Proposed Rulemaking, 35 FCC Rcd 7614, 7640, (2020), https://docs.fcc.gov/public/attachments/FCC-20-96A1.pdf, para. 80.

[93] Call Authentication Trust Anchor, WC Docket No. 17-97, Second Report and Order, FCC 20-136, (2020), https://docs.fcc.gov/public/attachments/FCC-20-136A1.pdf, paras. 79, 140.

[94] Protecting Consumers From One-Ring Scams, CG Docket No. 20-93, Notice of Proposed Rulemaking, 35 FCC Rcd 4908, (2020), https://docs.fcc.gov/public/attachments/FCC-20-57A1.pdf, para. 2.

[95] Call Authentication Trust Anchor, WC Docket Nos. 17-97 and 20-67, Report and Order and Further Notice of Proposed Rulemaking, 35 FCC Rcd 3241, 3292-96, (2020), https://docs.fcc.gov/public/attachments/FCC-20-42A1.pdf, paras. 123-130.

[96] Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, S. 151, 116th Congress, 2019, at § 14(a).

[97] Federal Communications Commission, "FCC Announces the Establishment of the Hospital Robocall Protection Group and Seeks Nominations for Membership," Public Notice, (released Mar. 25, 2020), https://docs.fcc.gov/public/attachments/DA-20-333A1.pdf.

- How providers can better combat unlawful robocalls made to hospitals.
- How hospitals can better protect themselves from such calls, including by using unlawful robocall mitigation techniques.
- How the federal government and states can help combat such calls.

The HRPG held its first meeting in July 2020. It recommendations are due in December 2020.

18.2 NANC CALL AUTHENTICATION TRUST ANCHOR WORKING GROUP

In February 2020, the FCC issued a referral letter to the NANC's CATA WG. It FCC directs the CATA WG to recommend best practices that will fulfill Congressional direction for the FCC to "issue best practices that providers of voice service may use as part of the implementation of effective call authentication frameworks . . . to take steps to ensure the calling party is accurately identified."[98]

The FCC directed the CATA WG to recommend best practices that address, at a minimum, six questions:

- Which aspects of a subscriber's identity should or must a provider collect to enable it to accurately verify the identity of a caller?
- What guidelines or standards should providers use when assigning the three attestation levels — A (or "full" attestation), B ("partial"), and C ("gateway") — of the STIR/SHAKEN framework?
- How should best practices vary depending on the type of subscriber, such as between large enterprises, individuals, and small businesses?
- When should providers consider using third-party vetting services, and how should they make the best use of them?
- Should there be unique industry-wide best practices for knowing the identity of subscribers located abroad? If so, what best practices could we recommend regarding identification of such subscribers?
- Are there any other best practices voice providers can implement "to take steps to ensure the calling party is accurately identified"?[99]

The NANC approved the CATA WG's report recommending best practices on September 24, 2020, and the FCC's Wireline Competition Bureau sought comment on those recommendations in October 2020.[100] The CATA WG was previously charged to investigate issues associated with the STIR/SHAKEN ecosystem and issued its Report on Selection of Governance Authority and Timely Deployment of STIR/SHAKEN in May 2018.[101] This report outlined recommendations for the establishment and selection of the STI-GA and STI-Policy Administrator (STI-PA).

18.3 STATE LEGISLATIVE ACTIVITY

As of this report, attempts to mitigate robocalls through state legislative activity have been largely unsuccessful. The following highlights the approach that some states have taken. These efforts may be indicative of what other states may be considering:

- Some states (Vermont and Tennessee) have proposed bills to tax robocalls, with the thought that the tax would encourage offending providers to lower call volumes and send only necessary calls.
- New York previously proposed a budget bill (A9508/S7508) in January 2020 that initially contained language with a January 1, 2021, STIR/SHAKEN implementation mandate for SP IP networks. The bills also included annual reporting requirements for CAs operating in the STIR/SHAKEN arena.[102] This language was removed from the bill prior to passage.[103]
- In February 2020, a bill was proposed in the Maryland legislature that would require VoIP providers to obtain specific contact and business information from persons placing robocalls through their networks.[104] This bill did not pass prior to the adjournment of the legislature.
- In October 2019, California signed into law SB 208, requiring that "on or before January 1, 2021, each telecommunications

[98] Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, S. 151, 116th Congress, 2019, at § 4(b)(l).

[99] Federal Communications Commission to Jennifer K. McKee, "Re: Call Authentication Trust Anchor Working Group," February 17, 2020, https://docs.fcc.gov/public/attachments/DOC-362809A1.pdf.

[100] Wireline Competition Bureau Invites Comment on Caller ID Authentication Best Practices, WC Docket No. 20-324, Public Notice, (released October 1, 2020), https://docs.fcc.gov/public/attachments/DA-20-1154A1.pdf.

[101] NANC Call Authentication Trust Anchor Working Group, Report on Selection of Governance Authority and Timely Deployment of SHAKEN/STIR, http://nanc-chair.org/docs/mtg_docs/May_18_Call_Authentication_Trust_Anchor_NANC_Final_Report.pdf

[102] State of New York, S. 7508, A. 9508, January 22, 2020, https://legislation.nysenate.gov/pdf/bills/2019/A9508.

[103] State of New York, S. 7508--B, A. 9508--B, https://legislation.nysenate.gov/pdf/bills/2019/S7508B.

[104] State of Maryland, House Bill 1278, Voice Over Internet Protocol – Robocalls – Customer Information, February 7, 2020, https://legiscan.com/MD/text/HB1278/2020.

SP shall implement STIR and SHAKEN protocols or similar standards to verify and authenticate caller identification for calls carried over an internet protocol network."

18.4 INTERNATIONAL

18.4.1 European Efforts

Europe recognizes the issue with robocalling and caller ID spoofing. The European Commission and national regulators are starting to take more of an interest given the FCC's regulatory response in the U.S. regarding SHAKEN. One of the primary considerations is regulatory jurisdiction (i.e., dealing with bad actors outside of Europe).

European SPs are taking action against robocalls, but so far, this mainly involves monitoring traffic at the edge of the network and at national borders to identify problem traffic. The big European international carriers are using algorithms in their networks to detect traffic patterns and sources. They are also looking at calls that appear to have national caller IDs coming in over international gateways and blocking those.

The European Conference of Postal and Telecommunications Administrations (CEPT) NaN2 (Number Portability, Switching, and Trust in Numbering) group is currently coordinating the European response. CEPT views several related problems as being at least as important today as robocalling and caller ID spoofing. These include:

- Toll fraud (e.g., call stretching).
- Changing the caller ID to make international calls look like they originate within the EU to avoid termination charges.

As a result, the EU is evaluating solutions other than SHAKEN (e.g., Stopping Exploitation of Internetwork Signaling by Mitigating Illegitimate Communications (SEISMIC)) to understand if they are competing or complementary solutions.

Below are some of the recent legislation driven efforts. There are additional activities not included where regulators are investigating approaches to robocalling and anti-spoofing, but those are less likely to be formalized prior to legislative support in their markets.

- France passed enhanced robocalling regulation in July 2020 requiring DNC enhancements for consumer blocking preferences and operator authentication of calling parties and calling numbers within three years. The regulator Autorité de Régulation des Communications Électroniques et des Postes (ARCEP) is investigating approaches appropriate for rulemaking including SHAKEN. This includes both voice and text messages.[105] [106]
- Germany is revising its communications act (Telekommunikationsgesetz (TKG)) to make it illegal to manipulate number transmission in signaling networks with an intent to do harm. Bundesnetzagentur (BNetzA), the German regulator, will follow with rulemaking accordingly.[107]
- The upcoming revision of the EU's Electronic Communications Code is expected to include provisions against CLI spoofing that will drive the remainder of the EU in the same direction.[108]

The prevailing view is that it may be better to step back and consider the full range of problems (e.g., robocalling, toll fraud) and deploy a solution that addresses multiple issues. There had been a belief that SHAKEN was purely a national-level concern. However, the interoperability between the U.S. and Canadian SHAKEN solutions has drawn attention to the possibilities, and there is a growing recognition that there may be value in a coordinated EU response. This will continue to be evaluated going forward. As of today, there is no movement to legislate SHAKEN, or even to mandate it through regulation, as it is in the US.

In the UK, OFCOM has been working on robocall mitigation since 2014 and with an industry consultative group since 2015. UK efforts have been centered on blocking based on analysis and traceback data. There has been a steady decline in complaints as these measures have become more effective. There does not seem to be great interest in using STIR/ SHAKEN in the UK at this time.[109]

[105] FR24 News, "The Law Against Telephone Canvassing in in Force Today," FR24 News, September 1, 2020, https://www.fr24news.com/a/2020/09/the-law-against-telephone-canvassing-is-in-force-from-today.html

[106] The law (in French) can be found at: https://www.legifrance.gouv.fr/download/pdf?id=CNSYRW_lXtGdOnnG84hvAostvrbVw7vibSlX3L_C8eE

[107] See Clause 66K. The Act (in German) can be found at: https://www.gesetze-im-internet.de/tkg_2004/.

[108] The Directive can be found at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972&from=EN

[109] Information Commissioner's Office and Ofcom, Nuisance Calls and Messages, May 4, 2020, https://www.ofcom.org.uk/__data/assets/pdf_file/0034/194974/nuisance-calls-joint-action-plan-2020.pdf

18.4.2 Canadian Industry Efforts to Implement STIR/SHAKEN

In April 2019, a group of Canadian SPs and the Canadian LNP Consortium, proposed the establishment of the Canadian Secure Token Governance Authority (CSTGA).[110] In December 2019, the Canadian Radio-television and Telecommunications Commission (CRTC) issued CRTC Compliance and Enforcement Decision 2019-403, which approves the CSTGA.[111]

This decision also requests that the industry group provide a progress report to the CRTC every six months. In 2019-403, the CRTC outlines expectations for the CSTGA:

- The CSTGA will establish a PA and one or more CAs.
- The CSTGA will participate in the CRTC Interconnection Steering Committee (CISC) to address STIR/SHAKEN implementation issues and ensure successful implementation by September 2020.
- The CSTGA will closely collaborate with Telecommunications SPs.[112]

In December 2019, CRTC issued a call for comments on a proposal that Canadian carriers and other telecom carriers that provide voice telecommunications in Canada be required to implement STIR/SHAKEN as a condition of providing services. This proposal would become effective in September 2020. Comments on Compliance and Enforcement and Telecom Notice of Consultation CRTC 2019-404 were due by January 27, 2020.[113] As of this report, the CRTC has yet to issue a mandate for STIR/SHAKEN.

18.4.3 Australia Communications Alliance Ltd Reducing Scam Calls Industry Code

The Reducing Scam Calls Working Committee of Australia's Communications Alliance Ltd. has developed an industry code aimed at identifying, tracing, and reducing the volume of scam calls. The working committee is comprised of representatives from the telecommunications industry and the Australian Communications and Media Authority (ACMA). The code is issued in draft form for public comment as DR C661:2020 REDUCING SCAM CALLS Industry Code,[114] which was due May 8, 2020. The code is to be submitted to the ACMA for registration under Section 117 of the Telecommunications Act 1997.[115] This work defines the process for "identifying, tracing, blocking and otherwise disrupting Scam Calls."

The processes developed in the code are built on improved information sharing between carriers/carriage SPs (C/CSPs), as well as improved information sharing between industry and regulators. Per the code, the key objectives include:

- Provide the definition of scam calls.
- Establish processes by which C/CSPs will work with each other and the regulators to identify and handle scam calls.
- Establish processes to share and communicate evidence of scam calls between C/CSPs and the regulators.
- Establish processes for C/CSPs to exchange information in order to trace the origin of scam calls.
- Establish a process for C/CSPs to block scam calls (from specific A-Party CLI(s).
- Establish a process to reinstate calls from blocked A-Party CLI(s).

18.4.4 Telecom Commercial Communications Customer Preference Regulations (Telecom Regulatory Authority of India)

In May 2018, the Telecom Regulatory Authority of India (TRAI) announced the draft Telecom Commercial Communications Customer Preference Regulations (TCCCPR), inviting written comments from stakeholders by June 11, 2018 (later revised to June 18, 2018). All clauses of the TCCCPR came into effect 150 days after the July 19, 2018, publication in the Official Gazette. The TCCCPR gives access SPs wide powers and responsibility to deal with unsolicited commercial communications in India[116] and is unique in its mandate to adopt DLT to achieve these goals.[117]

[110] TransNexus, "Canadian Regulator Announcements on STIR/SHAKEN," December 9, 2019, https://transnexus.com/blog/2019/crtc-shaken-announcements/

[111] CST-GA: Canadian Secure Token Governance Authority, "About," 2020, https://cstga.ca/.

[112] Canadian Radio-television and Telecommunications Commission, Compliance and Enforcement and Telecom Decision CRTC 2019-403, December 9, 2019, https://crtc.gc.ca/eng/archive/2019/2019-403.pdf

[113] Canadian Radio-television and Telecommunications Commission, Compliance and Enforcement and Telecom Notice of Consultation CRTC 2019-404, December 9, 2019, https://crtc.gc.ca/eng/archive/2019/2019-404.pdf

[114] Communications Alliance Ltd, Industry Code, C661:2020, Reducing Spam Calls, November 2020, https://www.commsalliance.com.au/__data/assets/pdf_file/0015/72150/C661_2020.pdf.

[115] Australian Government Federal Register of Legislation, Telecommunications Act of 1997, https://www.legislation.gov.au/Series/C2004A05145.

[116] Trilegal, "India: The Telecom Commercial Communications Customer Preference Regulations, 2018," Mondaq, September 7, 2018, https://www.mondaq.com/india/telecoms-mobile-cable-communications/732200/the-telecom-commercial-communications-customer-preference-regulations-2018.

[117] The TCCCPR is unique in its mandate to utilize Distributed Ledger Technology. Per Chapter V, 13: "[a]ccess Providers shall adopt Distributed Ledger Technology (DLT) with

18.4.4.1 Requirements

TCCCPR has several key requirements, including:

- Access providers should ensure that commercial communication on their networks only takes place using "registered header(s) assigned to the sender(s) for the purpose of commercial communication."[118]
- Senders registered for making commercial communication may not initiate calls with an auto dialer that "may result in silent or abandoned calls." Senders should notify originating access providers regarding their use of auto dialers and take steps to "maintain abandoned calls within limits provided for in these regulations or Code(s) of Practice."[119]
- Access providers should develop or cause to develop an ecosystem with a variety of functions that allow customers to register their preferences (consent and revocation) for commercial communications, and to regulate the delivery of the commercial communications in accordance with these preferences.[120]

TRAI will assess penalties on access providers that fail to curb unsolicited commercial communications. These "financial disincentives" increase with the number of violations, with the highest penalty not to exceed 7 million rupees (about $98,500) per month.[121]

As noted in the third bullet above, the TCCCPR requires access providers to develop a system that registers customer preferences regarding commercial communication. The Customer Preference Registration Facility (CPRF) will record consent and revocation of consent for specific choices (e.g., categories, mode of communication, time of day communication is received). The CPRF should also give customers a variety of modes (including a mobile app) to register, modify, or de-register preference for commercial communications.[122] Changes made by the customer should come into effect in near real time.[123]

18.4.4.2 Responsibilities of Access Providers

Access providers should develop code(s) of practice in accordance with the regulations of TCCCPR before allowing any commercial communication through its network. These codes cover registration of preference, complaint handling, detection, and monthly reporting, among other topics.[124]

The burden of ensuring that no unsolicited commercial communication is made to any recipient, except according to their preferences, is placed on the access provider. The access provider is also responsible for publicizing the customer's ability to register preference.[125]

18.5 OTHER INTERNATIONAL ISSUES

The SHAKEN standard "ATIS-1000074" specifies operation within the domain of a single national or regional regulatory authority. In most cases, this means within a single country. This was a conscious decision by the joint ATIS and SIP Forum IP-NNI Task Force (IP-NNI TF) to develop a solution that explicitly addressed U.S. requirements more quickly. However, SHAKEN does not assume unique U.S. attributes and should be equally applicable to other countries. Calls that originate in one country and terminate in another country are not explicitly addressed in the existing SHAKEN standard. This document provides a mechanism to extend the SHAKEN trust environment to include more than one country without requiring SPs to make changes to their current standard SHAKEN interfaces.

ATIS-1000087, Mechanism for Initial Cross-Border Signature-based Handling of Asserted information using toKENs (SHAKEN), specified a mechanism that allows countries with similar interests and regulatory environments to federate their SHAKEN infrastructure and extend the trust environment to include both countries. This specification only considers a bilateral arrangement between two jurisdictions, although it may be possible to extend this to include a limited number of additional countries. The more general solution for global interworking requires further study.

permissioned and private DLT networks for implementation of the system, functions and processes as prescribed in Code(s) of Practice: (1) to ensure that all necessary regulatory pre-checks are carried out for sending Commercial Communication; (2) to operate smart contracts among entities for effectively controlling the flow of Commercial Communication."

[118] Telecom Regulatory Authority of India, Telecom Commercial Communications Customer Preference Regulations, 2018, July 19, 2018, https://trai.gov.in/release-publication/regulations/amendments-page/96314, Chapter II, 3.

[119] Ibid, Chapter II, 4.

[120] Ibid, Chapter II, 5

[121] Ibid, Chapter VI, 27.

[122] Ibid, Chapter III, 6.

[123] Ibid, Chapter III, 7.

[124] Ibid, Chapter IV, 8.

[125] Ibid, Chapter IV, 10-11.

19

CONSIDERATIONS FOR FURTHER WORK

CONSIDERATIONS FOR FURTHER WORK

In lieu of regulation, TSPs — along with OSPs, analytics services, and industry organizations — may wish to work toward developing recommendations and best practices that provide guidance yet allow for flexibility and maintaining fair competition.

19.1 ORIGINATOR REGISTRATION

Originators should register their phone numbers with available call registries and analytics services should take that information as data points into consideration for call disposition and labeling.

19.2 NO GUARANTEED DELIVERY OF SHAKEN PASSPORTS

In many cases, routing of phone calls between an OSP and TSP happens through multiple intermediary SPs. Routes may change dynamically based on a variety of factors, including price, commercial concerns, availability, and other technical factors. Even if an OSP originates and exchanges all calls with SHAKEN PASSporTs over IP, there is no guarantee that the TSP will receive the SHAKEN PASSporT intact. One key reason is the practice of exchanging calls using non-IP technologies (TDM based) or IP infrastructure that has not been upgraded to support PASSporTs.

To facilitate the guaranteed delivery of SHAKEN PASSporTs, multiple avenues should be explored.

19.2.1 Further Study and Standardization of Out-of-Band Delivery of SHAKEN PASSporTs

The industry has begun to examine this issue. This work should continue and be expedited.

19.2.2 Further Study on Call Authentication Technologies for Non-IP Technologies

Because many calls are transmitted over non-IP networks, further study of how call authentication can traverse non-IP technologies should be carried out. ATIS has initiated work on this issue through its Non-IP Call Authentication Task Force.

19.2.3 Further Study on Regulation and Other Government Measures to Ensure Transit of Calls with Call Authentication Intact

The exchange of calls within the U.S. is regulated by the FCC to ensure fair access and competition in the U.S. telecom market. Existing rules may be reviewed to improve the exchange of calls with call authentication intact to ensure fair access to the North American telecom market. The key authentication technology behind SHAKEN PASSporTs can also be used to exchange other critical call parameters such as priority requests from authorities and other enhancements that would be key to modernize the North American telecom market.

19.3 FAIR ACCESS TO IDENTIFICATION IN THE TELEPHONY NETWORK

While SHAKEN PASSporTs properly authenticate that the originator has the right to use the calling number, many services — such as CNAM and other similar device application technologies — augment the calling number with additional information about the caller such as the name, potential geographical area, and even logos. Technical standards and regulation should be developed and/or extended to allow for fair access to identification of callers in the network.

19.3.1 Further Study of Technologies for Digital Identity in the Telephony Network

Digital identification technology is increasingly being used across society to authenticate communications between individuals and enterprises alike. Further studies should investigate how digital identities and their associated technologies could be used in the telephony network to carry identity information, authenticate ownership/control of numbering resources, and augment analytics of call use cases. Additionally, the option of using existing digital identity sharing technologies to provide fair and equal access to identity information using technologies like DLTs should be studied.

19.3.2 Further Study on the Integrity of Caller Identity and CNAM Information

Authoritative CNAM databases are distributed databases that host virtually all working phone numbers (landline and wireless). Accessing these databases, however, is transparent to the end users and their SPs. Network protocols handle routing to the appropriate database. Collectively, these databases act as a single national database. Each record in the database stores the TN, the associated name, and more.

Consumers have relied on these databases for more than 20 years to manage their calls, and SPs have had and continue to have fair access to authoritative databases. Given SHAKEN call authentication and its promise of minimizing call spoofing, the accuracy of authenticated calls becomes an important source of the authenticated identity. Any indication of the authenticity of the calling number will likely be perceived by the called party as extended to any displayed name. Recently, with the rise of alternative CNAM data sources, via non-authoritative databases or SIP signaling, the industry needs to focus on the integrity of the CNAM data being delivered to the consumer.

Database providers wanting to be a player in the caller identity ecosystem should follow best practices to verify that the TN holder is authorized to use the stored name and its associated metadata (e.g., logo). Best practices should include the near-real-time updates to changes in the data and ongoing audits of the data. The industry must guard against repeating past mistakes of creating opportunities that bad players could exploit (e.g., paying to deliver any name and logo that facilitates defrauding consumers) while allowing individuals and organizations to be accurately and uniformly represented using CNAM.

It is also the SPs' responsibility to carefully evaluate and select the sources (RCD or databases) used for delivering CNAM and metadata (such as enhanced CNAM or eCNAM) to their end users. Retrieving data from less trustworthy sources continues to facilitate defrauding the American public.

A study should be conducted on best practices/ industry guidelines on:

- Vetting requirements for authoritative user data and similar information such as RCD that are used to identify the caller and calling purpose, complementing vetting requirements for STIR/SHAKEN authentication.
- Whether to require SPs (including wireless SPs) to use an authoritative database designated by the TNSP for CNAM and similar information.
- Timeliness of updates for authoritative data and RCD.
- Policies to ensure accurate information for authoritative databases and RCD.
- Exploring possible incentives around eCNAM/RCD and associated metadata information to prevent exploitation of these data sources.
- Whether eCNAM/RCD and associated metadata information should influence analytics treatment.

Because RCD and eCNAM/CNAM provide similar services, the study should clarify how these two mechanisms can coexist, whom the trust anchors should be, and the requirements and policies for both mechanisms.

19.3.3 Further Study of Know-Your-Customer Regulation and Industry Collaboration

A precondition for STIR/SHAKEN's success is the ability to provide A-level attestation for calls. This means that the OSP has sufficient knowledge about the customer's identity and knows that the customer has the right to use the calling number. In a coalition with relevant authorities, the industry should define the minimal set of KYC information that must be collected, including any requirement for record retention and vetting procedures. Many SPs may be challenged to orchestrate the proper collection of KYC information, as well as the proper vetting of said information. So, the industry and regulators should identify technical and administrative standards and procedures to facilitate sharing of vetted KYC information, perhaps using digital certificate technologies and trusted service bureaus that could facilitate this for the industry. Standardization and sharing of certification would greatly benefit enterprises, which would be able to re-use a vetted identity and credentials across multiple vendors.

19.4 FAIR TREATMENT OF ANALYTICS

While serving an important role to block and label illegal robocalls, analytics services also carry a significant risk in mislabeling or blocking important and legal calls from authorities and enterprises.

While the further study on continued improvements is recommended, the FCC has given examples of objective standards it considers part of reasonable analytics services and declined to define further.[126] Thus far the FCC has declined to require providers to provide an error code to the calling party. But it requires providers to maintain a single point of contact to resolve unintended or inadvertent blocking[127] and is defining effective redress options for callers as per the TRACED Act.[128]

Therefore, further discussions should include focusing on empowering analytics services to improve their algorithms and solution. For example, topology hiding makes the job for analytics services more complex. Carriers also walk a fine line between network security and useful call information available to analytics services.

[126] Advanced Methods to Target & Eliminate Unlawful Robocalls and Call Authentication Trust Anchor, FCC No. 19-51, CG Docket No. 17-59, WC Docket No. 17-97, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, (released June 7, 2019), para. 35

[127] Advanced Methods to Target and Eliminate Unlawful Robocalls, FCC No. 20-96, CG Docket No. 17-59, Third Report and Order, Order on Reconsideration, and Fourth Further Notice of Proposed Rulemaking, (released July 27, 2020), para. 54.

[128] Ibid, para. 51.

Uniform analytics and overly defined regulations actually help bad actors learn how to avoid detection, so the industry should only work toward common guidelines. Further study should include high-level fundamental requirements and processes any solution should address.

19.4.1 Further Study of Regulation of Rights for Call Originators

Further study should be conducted on the regulation of the rights and procedures for known call originators to:

- Be informed of any labeling or blocking occurring.
- Remediate any mislabeling or wrongful blocking.

The impact of this on the ability of illicit callers to refine their illegal calling techniques needs to be part of any study.

19.4.2 Study of Identification of Call Originators for the Public Good

Schools, local governments, health authorities, and NGOs serving similar purposes all need to use the telephony network to reach the public. The recent COVID-19 emergency has put a spotlight on this need. Because many of these use cases may be flagged by analytics services to be either illegal or nuisance calls, it is important to provide these actors with a way of clearing their calls. A study should be conducted on how best to solve this problem (e.g., create a registry of call originators where terminating SPs can find an authoritative source of calling numbers and their corresponding CNAM).

The industry may still consider an organized source for critical call numbers to achieve these goals, which could be helpful, but must be coupled with STIR/SHAKEN and robust analytics. As the STIR/SHAKEN scope evolves, originators of critical calls should fall under the umbrella. Protection of their numbers will be enhanced if they register their numbers with registry services so this extra information is taken into consideration by their service engines.

20

REFERENCED INDUSTRY ORGANIZATIONS

REFERENCED INDUSTRY ORGANIZATIONS

The following list includes the standards and industry organizations that are referenced in this document:

- 3rd Generation Partnership Project (3GPP)[129]
- Internet Engineering Task Force (IETF)[130]
- SIP Forum[131]
- Risk & Assurance Group[132]
- Messaging Malware Mobile Anti-Abuse Working Group (M3WAAG)[133]
- Australia Communications Alliance Ltd[134]
- USTelecom Industry Traceback Group[135]

[129] https://www.3gpp.org/

[130] https://www.ietf.org/

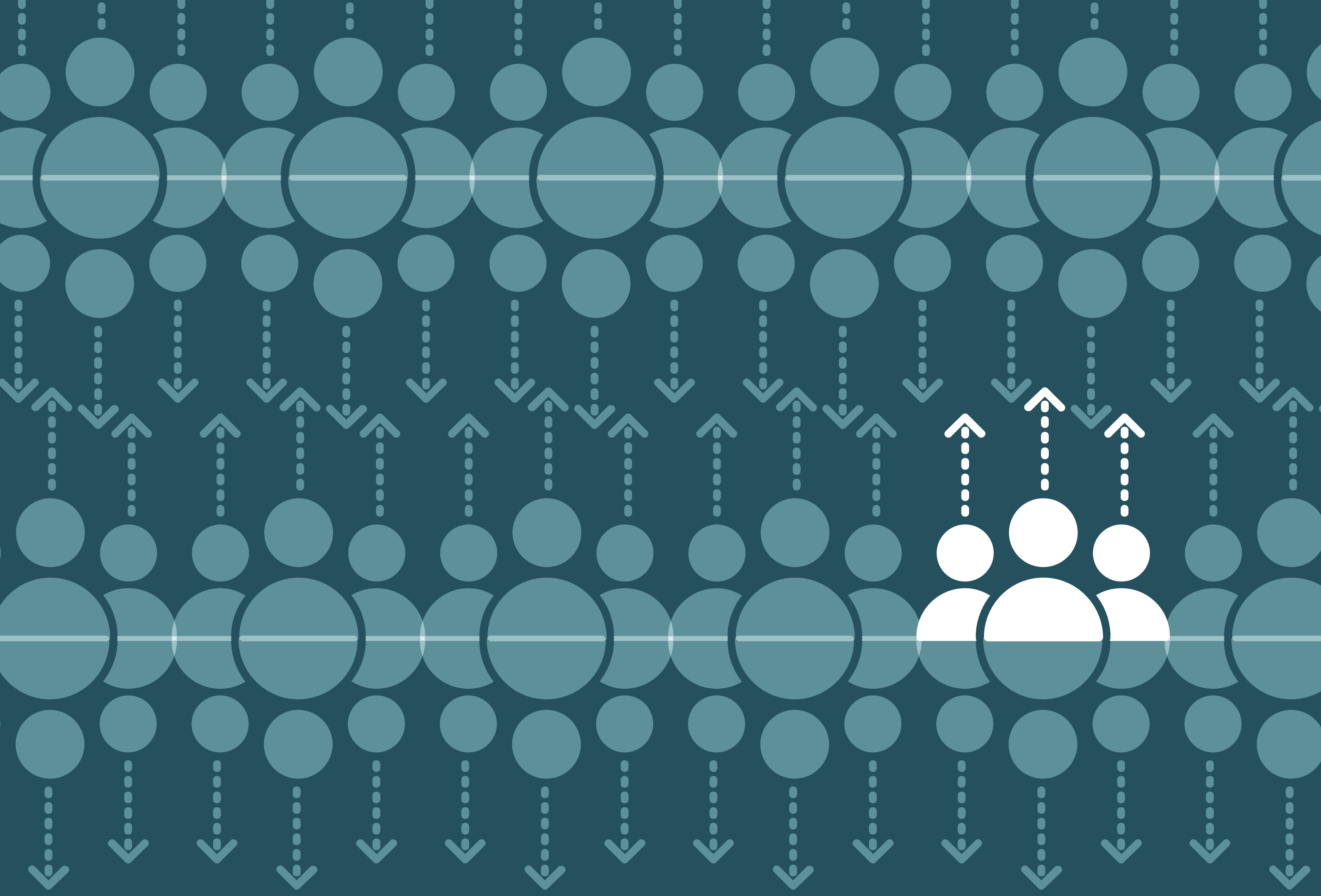
[131] https://www.sipforum.org/

[132] https://riskandassurancegroup.org/

[133] https://www.m3aawg.org/

[134] https://commsalliance.com.au/

[135] https://www.ustelecom.org/the-ustelecom-industry-traceback-group-itg/



21 CONTRIBUTORS TO THIS REPORT

CONTRIBUTORS TO THIS REPORT

Amazon Web Services

AT&T

Bell Canada

Comcast

Hiya

Ericsson

First Orion

GBSD Technologies

Hiya, Inc.

iconectiv

Inteliquent

Intrado

Lumen

Mediacom Communications, Inc.

Neustar, Inc.

Nokia

Numeracle

Oracle

Sprint

TDS

Telnyx

T-Mobile USA

Transaction Network Services

Twilio

USTelecom

Verizon

YouMail

APPENDIX

APPENDIX A

Representative Sample of Network Call Blocking and Labeling Services

This appendix represents a sample of call blocking services and their availability at the time of this report, some of which are available free of charge.

Service	Description
AT&T Call Protect, free[136] Call Protect Plus	AT&T's Call Protect app is available for iOS and Android. The free version blocks calls from "likely fraudsters" and labels telemarketing calls. You can add numbers to a block list in the app as well. The paid version provides caller ID for unknown numbers and offers mobile security features that are unrelated to robocalls.
AT&T Digital Phone Call Protect, free[137]	AT&T's Digital Phone Call Protect includes features such as automatic fraud blocking, call blocking, and suspected spam call warning.
First Orion[138]	First Orion offers Call Protection and Call Enhancement solutions for businesses, organizations and carriers: • STIR/SHAKEN - standards-based implementation of STI-AS, STI-VS, STI-KMS, STI-CR, and STI-KMS, and SKS. Standalone service or in conjunction with call protection and/or call enhancement services. • Complete call analytics suite including the CallPrinting spoof mitigation solution. All services are extremely flexible, supporting a range of call disposition options and preferences, and allowing operators to implement their own unique business rules. Rich call enhancement suite of services including CNAM, flexible Inform for enterprises and organizations, and Engage for a truly personalized calling experience: name, logo, reason for calling, rich graphics, and more. All call enhancement options work with call protection and spoof mitigation solutions, as well as with STIR/SHAKEN.
Neustar Robocall Mitigation service (RM)[139]	Neustar offers a suite of trusted call solutions for both carriers and enterprise customers. The Robocall Mitigation service (RM) provides carriers and MSOs with an enhanced overlay of Neustar's CNAM solution's database information, including advanced analytics for detection of fraudulent robocaller calls from, and proactive alerts of suspected fraudulent calls to the called party.
Neustar Caller Name Optimization (CNO)[140]	The Caller Name Optimization (CNO) solution provides enterprises with tools to directly manage the name and brand content associated with their TNs for CNAM presentation to over 850 operators. This verified call originator data – whether outbound, inbound, or DNO – is then registered with network operators and/or their analytics services for consideration in their analytics models toward mitigation of call blocking and spam-labeling of legitimate businesses.
Neustar Certified Caller (CC)[141]	The Certified Caller (CC) solution is a standards-compliant solution that provides carriers and enterprises with the ability to sign and verify telephone calls using STIR, the associated standards developed by the IETF, and SHAKEN, the framework developed by ATIS and includes: • STI-AS – Secure Telephone Identity – Authentication Service • STI-VS – Secure Telephone Identity – Verification Service • STI-DB – Secure Telephone Identity – Database • STI-CR – Secure Telephone Identity – Certificate Repository • STI-KMS – Secure Telephone Identity – Key Management Service
Neustar Branded Call Display (BCD)[142]	The Branded Call Display (BCD) solution extends the suite of Trusted Call Solution capabilities to deliver an enhanced, personalized, and contextual call experience. It includes the ability for enterprises to enhance their caller identity with a customized brand display (e.g., name, business location, call intent) enriched with logos, images, and the call authentication/verification result in a rich multimedia display.
T-Mobile Scam Shield™[143]	T-Mobile's Scam ShieldTM is free to all customers and includes Scam Block. The ID portion of the service will alert you that an incoming call is likely spam, while Scam Block will block the call from ever reaching your phone.
Verizon Call Filter, free[144] Call Filter Plus	Verizon's Call Filter app is automatically enabled for Android users on a postpaid plan. The service offers spam detection, a spam filter, and the option to report numbers for free. Call Filter Plus additionally includes caller ID, spam lookup, and a personal block and spam list.

[136] www.att.com/features/security-apps/

[137] https://www.att.com/support/article/u-verse-voice/KM1235421/

[138] https://firstorion.com/

[139] https://www.home.neustar/caller-intelligence/robocall-mitigation

[140] https://www.home.neustar/caller-intelligence/certified-caller

[141] https://www.home.neustar/branded-contact-management/caller-name-optimizationv

[142] https://www.home.neustar/branded-contact-management/branded-call-display

[143] https://www.t-mobile.com/customers/scam-shield

[144] https://www.verizon.com/solutions-and-services/call-filter/

YouMail and YouMail Data Solutions[145]	The YouMail call protection app is available for free on iOS and Android for any US carrier. It can automatically block robocalls, spam, scam and fraud calls and messages as well as manage their own custom blocklists or allowlists. The app provides other free and paid communications features. YouMail Data Solutions provide real-time embeddable or queryable data solutions for SPs, enterprises, and contact centers to better identify, as well as block the unwanted calls entering or exiting their networks.

APPENDIX B

Representative Sample of Smartphone Blocking Applications

This appendix represents a sample of smartphone blocking applications and their availability at the time of this report, some of which are available free of charge.

Service	Description
Hiya Caller ID and Block App[146]	The Caller ID and Block Application has been available on Android and iOS for some time now. It's the same company that powers AT&T's Call Protect app, as well as Samsung's built-in call block and spam protection service. Samsung Galaxy users can enable the built-in service in the phone app.
Nomorobo[147]	Nomorobo was one of the winners of the FTC's RoboCall Challenge in 2013. Verizon uses Nomorobo for its Fios users, but it also has a phone app.
RoboKiller[148]	RoboKiller was the winning submission of Teltech systems (the makers of Trapcall) for the FTC Robocall: Humanity Strikes Back Contest in 2015.
YouMail[149]	Originally a cloud-based visual voicemail service that began in 2007, YouMail began providing its app for both Android and iOS in 2009.

[145] https://www.youmail.com/

[146] https://hiya.com/downloads

[147] https://www.nomorobo.com

[148] https://www.robokiller.com

[149] https://www.youmail.com