Robocall Strike Force Report

October 26, 2016

Executive Summary

Robocalls and telemarketing calls are currently the number one source of consumer complaints at the FCC. What was once a nuisance has become a plague to U.S consumers receiving an estimated 2.4 billion robocalls (1) per month in 2016.

The FCC has been encouraging service providers to offer call blocking solutions that give customers greater control over the types of calls they receive. Call blocking is one part of the robocall solution. Another part is identifying the bad actors who use robocalls to take advantage of unsuspecting consumers by using numbers assigned to others (spoofing). They use cheap and accessible technologies to spoof their caller identity and scam victims with threats from the IRS, offers of loans, or free travel. The Strike Force is committed to protecting customers, but these disguised calls have put investigators and enforcers at a disadvantage.

Although several providers and third parties offer call blocking and caller identification verification products, there is no ubiquitous solution that spans wireline and wireless communication networks. The industry has been called to action by the Robocall Strike Force to collaborate on creative solutions to this ever changing problem.

Mission Statement

The mission of the cross industry Strike Force is to accelerate the development and adoption of new tools and solutions to abate the proliferation of illegal and unwanted robocalls, to promote greater consumer control over the calls they wish to receive, and to make recommendations to the FCC on the role government can play in this battle.

Vision of Success

Success over illegal and unwanted robocalls requires action over three areas: source authentication, network and consumer blocking tools, and effective enforcement with the power to traceback and shut down offending accounts. The tools incorporating this technology will ultimately give customers the power to choose what types of calls they wish to receive and what to block. Finally, consumers have the opportunity to become aware of and learn to use these measures.

Affirmation Statement

As members of the Robocall Strike Force, we support the findings of this group, and will work with and support, as appropriate, efforts of standards bodies and other groups to facilitate the completion of the long term deliverables. Nothing in this document precludes any Strike Force

(1) https://www.youmail.com/phone-lookup/robocall-index/2016/june

member from advocating those policies and implementing those robocall mitigation efforts that each considers most effective and appropriate for its customers.

Strike Force Members

AT&T	Apple	Bandwidth.com	Birch
Blackberry	British Telecom	CenturyLink	Charter
Cincinnati Bell	Comcast	Cox	Ericsson
FairPoint	Frontier	GENBAND	Google
Inteliquent	Level 3	LG	Microsoft
Nokia	Qualcomm	Rogers	Samsung
SilverStar	Sirius/XM	Sprint	Syniverse
T-Mobile	US Cellular	Verizon	West
Windstream			

Getting Started

In his July 26, 2016 blog, Chairman Wheeler asked the industry to "develop an action plan for providing consumers with robust robocall-blocking solutions". On August 19, 2016, a 60-day Strike Force was created to meet the Chairman's request. The Strike Force created work groups to facilitate the collaboration across the telecommunications ecosystem. The work groups arranged around the four categories indicated below, and met at least twice per week over the last 60 days. The teams have developed short and long term deliverables to address unwanted and illegal robocalling, the details of which are provided below.

There is no silver bullet to solve the robocalling problem. Fraudulent robocallers constantly change their methods to bypass blocking solutions as they are implemented. Like the approach to cyber-attacks, our approach to unwanted and illegal robocall blocking needs to be constantly evolving and adapting. The work group solutions were created with this in mind.

Work Groups

Authentication	Empowering Consumer Choice	Detection, Assessment, Traceback, and Mitigation	Regulatory Support/Root Cause Removal

Consumer Benefits

Authentication:

The Strike Force accelerated, from December to October, the standards to verify and authenticate caller identification for calls carried over an Internet Protocol (IP) network. These standards are known as SHAKEN (Signature-based Handling of Asserted information using toKENs) and STIR (Secure Telephony Identity Revisited). The development and implementation of the standards after the 60-day term will continue through the Internet Engineering Task Force (IETF), Third Generation Partnership Project (3GPP) and Alliance for Telecommunications and Industry Solutions (ATIS) Session Initiation Protocol (SIP) Forum.

Consumer Benefit The deployment of these standards under a sound governance framework will result in higher end user confidence in the identification of incoming IP-only voice calls.

Empowering Consumer Choice:

Robocall Strike Force members from across the telephony ecosystem came together to provide the end user with a greater degree of identification and control over the types of calls they receive. To address the short term need for call blocking solutions, the group developed a plan to educate consumers on the capabilities existing in the market. To address longer-term needs, this group has recommended that standards groups develop an information flow, consumer presentation, and consumer-directed call disposition control options, as well as a framework for deploying resulting solutions. These will give consumers a clearer picture of the type of calls they are receiving, and expand their automatic and manual call handling options.

Consumer Benefit

Created awareness campaigns to educate consumers on existing blocking technologies in the short term and developed an environment where additional capabilities can be developed to facilitate consumer choice.

Detection, Assessment, Traceback, and Mitigation:

This group investigated various methods of detection and avoidance to stop unwanted calls from reaching customers by blocking at various network levels. This group has initiated a trial to block known numbers that should never originate traffic. The results of this trial will determine the viability of a Do Not Originate list of numbers to be blocked network wide in the future.

Consumer Benefit

Today, loopholes in the Publicly Switched Telephone Network are being exploited by bad actors to harm consumers. Strike Force members have established industry guidelines to enhance detection, traceback, and blocking of malicious traffic.

Regulatory Support/Root Cause Removal:

This group has supported the Robocall Strike Force's technical working groups by giving guidance about key terminology and the legal landscape, and by helping to remove regulatory roadblocks. They also have developed recommendations for actions the FCC can take to support industry efforts to trace back and to block illegal robocalls.

Consumer Benefit

It is in the public's best interest for government and industry to collaborate on the robocall problem. Government can ensure that industry has the flexibility to use robust tools to address illegal traffic on its own and industry can facilitate government efforts to investigate and shut down the illegal robocall operations that are the root cause of the problem.

Record of Strike Force Efforts

Work Group	Meetings	Contributors
Authentication	16	75
Empowering Consumer Choice	24	58
Detection, Assessment, Traceback, and Mitigation	24	70
Regulatory Support/Root Cause Removal	22	42
Miscellaneous meetings	12	____

1. Authentication Work Group

Co-Chairs: Chris Wendt, Comcast / Martin Dolly, AT&T

The Strike Force accelerated, from December to October, the standards to verify and authenticate caller identification for calls carried over an Internet Protocol (IP) network. These standards are known as SHAKEN (Signature-based Handling of Asserted information using toKENs) and STIR (Secure Telephony Identity Revisited). The development and implementation of the standards after the 60-day term will continue through the Internet Engineering Task Force (IETF), Third Generation Partnership Project (3GPP) the Alliance for Telecommunications and Industry Solutions (ATIS) Session Initiation Protocol (SIP) Forum, and the IP Network-to-Network Interconnection Task Force. The details of the Authentication team's work are outlined below.

Consumer Benefit The deployment of these standards will result in higher end user confidence in the identification of incoming calls for VoIP.

Section	Task	Estimated Date	Group
Authentication			
Short Term			
1.10.1	Internet Engineering Task Force (IETF) has given last call date of late October for feedback .	October 31, 2016	N/A
1.10.1	ATIS-SIP Forum SHAKEN framework approved for Letter Ballot, timeframe was accelerated from December to October 5th, 2016 providing an approved implementation profile for service providers using STIR.	October 5, 2016	N/A
1.10.2	Service requirement change requests for signaling from the network to the mobile device was agreed to at the August SA1 3GPP meeting, approval confirmed at the September SA Plenary meeting.	September 15, 2016	N/A
1.10.2	Discussion Paper and Change Request to 3GPP CT1 for modifications to 3GPP TS 24.229 for signaling Verification Information from the network to the device in the call/session setup signaling to be contributed to their October 17th meeting.	October 21, 2016	N/A
1.10.3	Submitted fast-track technical review on SS7 feasibility to Alliance for Telecommunications Industry Solutions (ATIS).	October 3, 2016	N/A
1.10.3	The Strike Force has reviewed the recommended options to extend authentication and verification interworking through SS7 to TDM/POTS service and has made recommendations.	October 7, 2016	N/A
1.10.4	Lab to Lab authentication prototype testing has been initiated between AT&T and Comcast.	August 30, 2016	N/A
1.10.4	ATIS has agreed to further progress work on testbed for authentication prototype testing.	November 1, 2016	ATIS
1.3	ATIS has agreed to further progress the authentication development and implementation roadmap.	October 26, 2016	ATIS and the SIP Forum's IP-NNI Task Force
1.8	ATIS has agreed to further progress the Signaling Verification and Analytics Information, and display framework.	October 26, 2016	ATIS and the SIP Forum's IP-NNI Task Force
1.7.5	ATIS has agreed to further progress the certificate governance and policy framework	October 26, 2016	ATIS and the SIP Forum's IP-NNI Task Force
Long Term			
1.10.7	ATIS has agreed to further progress certificate based authentication for further standards development with vendors, carriers, and OEMs.	January 2, 2017	ATIS
1.10.6	IETF WGLC of spam-info and unwanted draft RFCs.	April 2017	IETF
1.9.1	SIP Call Information Spam Call-Info and unwanted encodings into 3GPP CT1	January 2017	3GPP
1.10.4	SHAKEN Best Practices & additional STIR use cases.	Underway	ATIS and the SIP Forum's IP-NNI Task

1.1. IETF STIR and SHAKEN Overview:

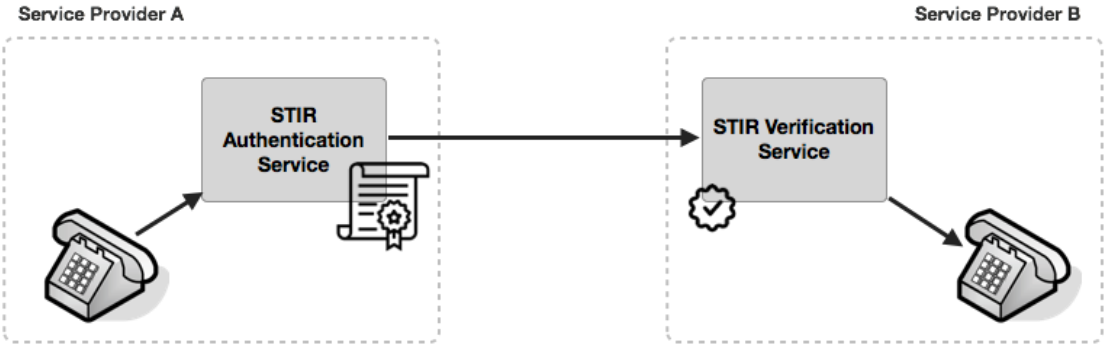
1.1.1. The protocols and specifications defined in the IETF STIR working group form the basis of the SHAKEN industry framework being developed in ATIS/SIP forum NNI Task Force.

1.1.2. The premise of STIR/SHAKEN is that telephone calls and the telephone numbers associated with the calls, when they are originated in a service provider network can be authoritatively and cryptographically signed by the authorized service provider, so that as the telephone call is received by the terminating service provider, the information can be verified and trusted.

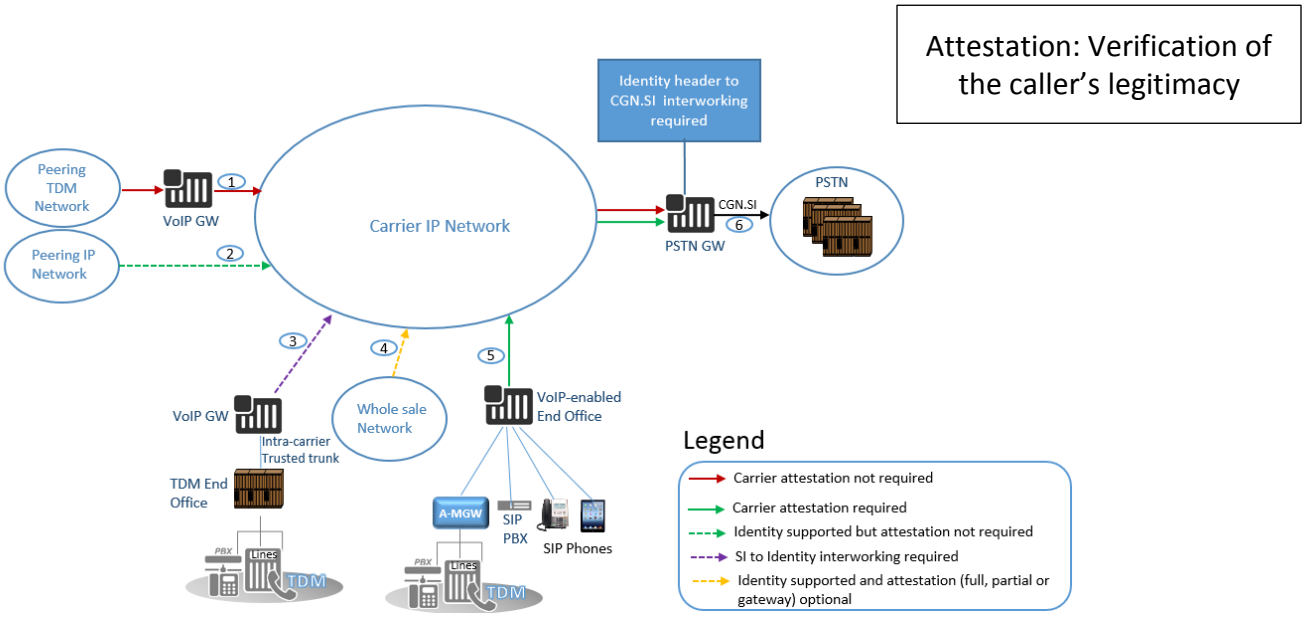
1.1.3. This set of industry standards is intended, as it is more fully deployed into the VoIP based telephone network, to provide a basis for verifying calls, classifying calls, and facilitating the ability to trust caller identity end to end. Illegitimate actors can then be more easily and quickly identified with the hope that telephone fraud is reduced significantly.

1.1.4. While industry members believe that the SHAKEN framework holds considerable promise for repressing the presence of robocalling in the communications ecosystem, the Strike Force recognizes that the nature of bad actors and their tactics to harass consumers with unwanted robocalls and fraudulent, spoofed Caller IDs are ever changing and adapting. Further, carriers are at various stages of transitioning to IP-enabled networks and SHAKEN fundamentally depends upon IP network technologies.

STIR/SHAKEN framework basic flow



1.2. Scope of SHAKEN Attestation and Feasibility of Screening Indicator (SI) Interworking



① Attestation not required for calls from peering network via Time Division Multiplexed (TDM) trunk since the Screening Indicator (SI) is not defined for this use.

② For calls from peering Internet Protocol (IP) network, Identity header shall be forwarded on if received.

③ Calls originated by subscribers served by the carrier via a legacy switch will have a reliable Screening Indicator. Hence, where feasible the carrier should provide attestation of the originator if the Screening Indicator is "network provided" or "user provided, verified and passed".

④ For calls from wholesale network, Identity header shall be forwarded on if received. If no Identity header is received the wholesale network may create a new Identity header with either full, partial or gateway attestation.

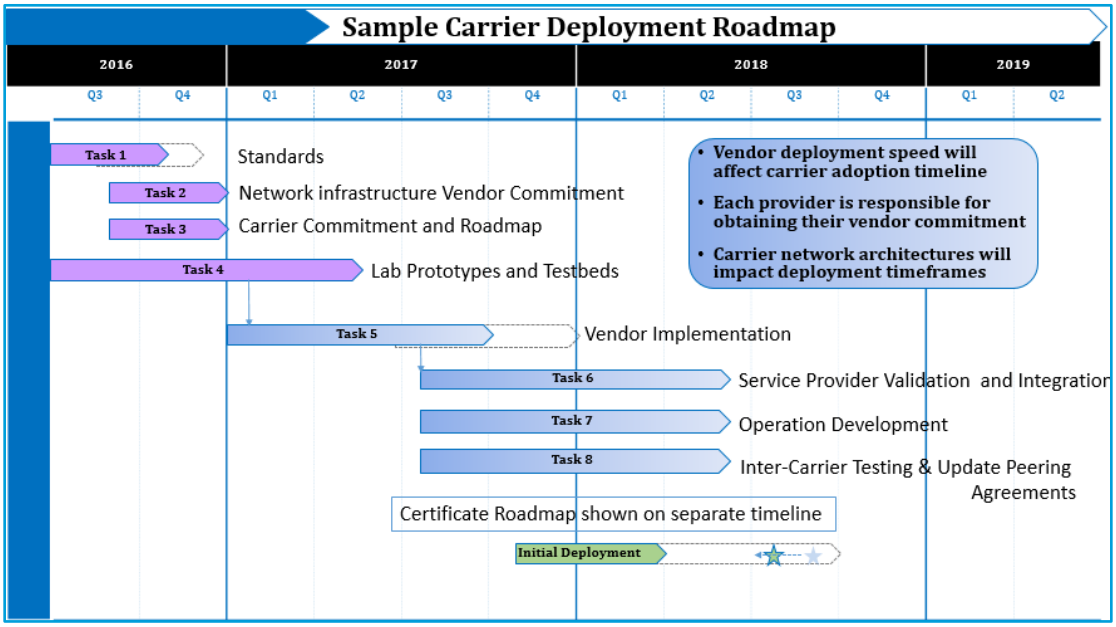
⑤ For calls originated by carrier owned subscriber via a Voice over Internet Protocol (VoIP) enabled end office, the carrier shall provide attestation for the originator.

⑥ This includes the scenarios where the originator is still on legacy wireline access equipment. If the originator is on a Private Branch Exchange (PBX), the carrier should where feasible provide call screening. If screening is successful, attestation should be provided.

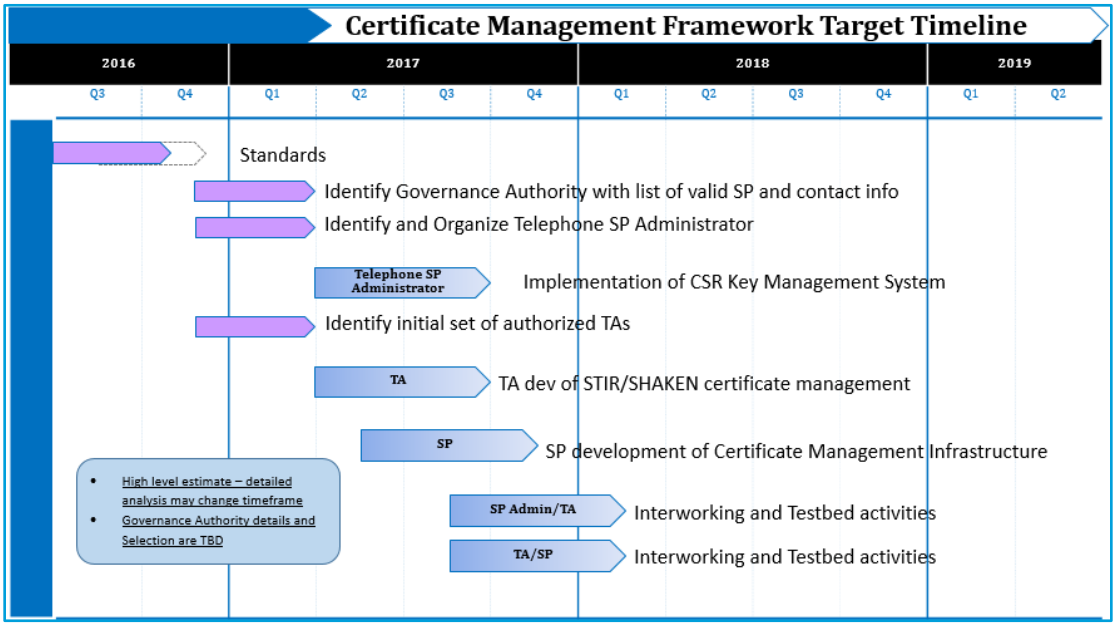
Note: The definitions and explanations in the above bullets for Section 1.2 are consistent with existing standards documents.

1.3. Sample Carrier Deployment Timeline

The Implementation of STIR/SHAKEN will vary by carrier and network type



1.4. Certificate Management Framework Target Timeline



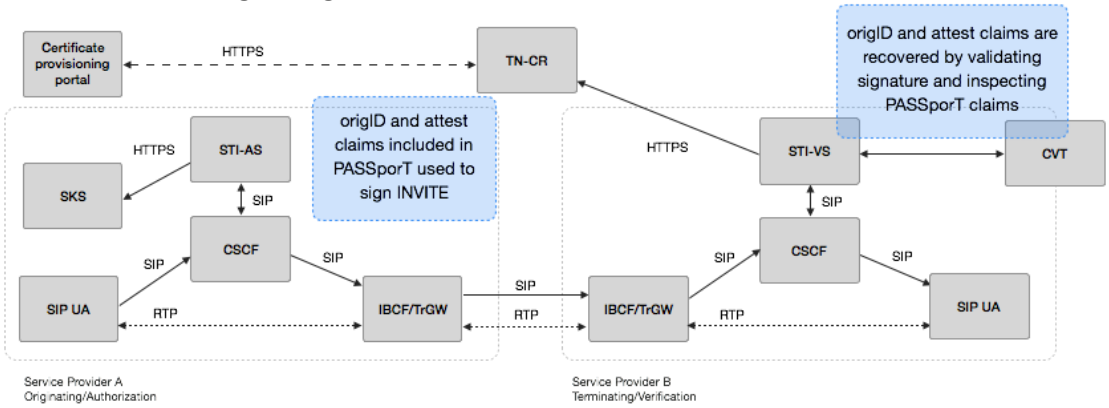
1.5. SHAKEN attestation and originating identifiers

1.5.1. SHAKEN and the “shaken” PASSporT extension define the ability for the service provider originator to sign the call using claims that represent an attestation (“attest”) and unique originating identifier (“origid”).

1.5.2. The attestation provides the verifier with information on the origination of the call and attestation level the originating provider is giving the calling identity.

1.5.3. The originating identifier is useful for both ease of trace back to more granular levels beyond the service provider signing the token and can provide a consistent indicator to analytics for reputation and other metrics.

Attestation and Originating Identifier call flow



1.5.4. Attestation- The service provider will classify the origination of the call into three categories:

- **Full Attestation:** The signing provider:
  - is responsible for the origination of the call onto the IP based service provider voice network.
  - has a direct authenticated relationship with the customer and can identify the customer.
  - has established a verified association with the telephone number used for the call.
- **Partial Attestation:** The signing provider:
  - is responsible for the origination of the call onto its IP based voice network.
  - has a direct authenticated relationship with the customer and can identify the customer.
  - has NOT established a verified association with the telephone number being used for the call.
- **Gateway Attestation:** The signing provider:
  - is the entry point of the call onto its IP based voice network.
  - has no relationship with the initiator of the call (e.g., international gateways).

1.5.5. Originating Identifier:

- This is a unique and opaque UUID (RFC4122) that will be used for two reasons:
  - Traceback identification of originator, either service provider, wholesale customer, enterprise
  - By verification and call spam classification/analytics as an opaque identity to associate reputation scores and identify bad actors to authorities for potential follow up

1.6. VoIP Traceback

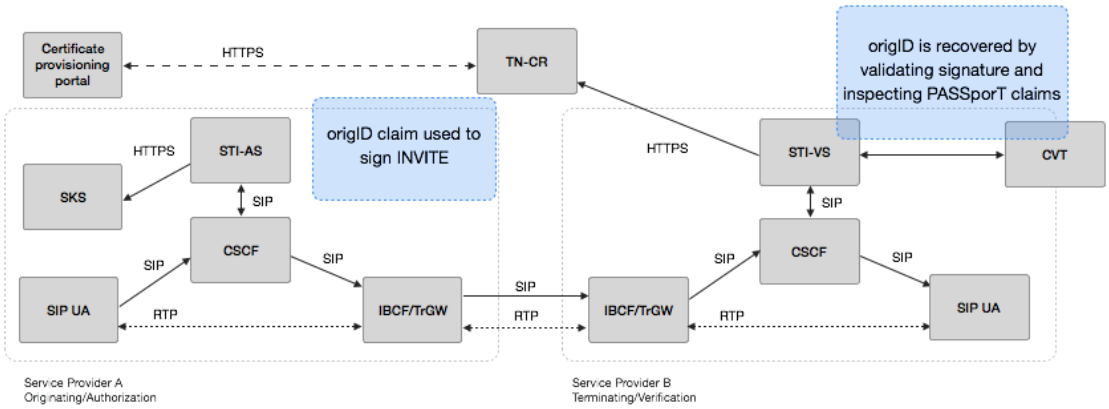
1.6.1. SHAKEN defines a framework of the use of digital signatures created either at the origination network of the authenticated device, or in the case of TDM to VoIP, at the gateway that the call enters the VoIP network.

1.6.2. Traceback procedures today are cumbersome in terms of manual investigation of call logs hop by hop.

1.6.3. SHAKEN has defined a unique Originating Identifier (origid) which has been specifically incorporated to make traceback an easy and automatic process, specifically identifying beyond the service provider that originated the call, the specific service provider customer

or gateway node that the call was signed. This Originating Identifier is specifically designed to be opaque, so that there is not any directly identifiable information available in the SIP INVITE. However, in an authorized traceback request, the service provider can be queried to get any required information needed for enforcement activities.

Example call flow with origid



1.6.4. Traceback procedures for VoIP:

- The intent of VoIP traceback is that it becomes a fully automated way of notifying providers of potential bad actors.
- The more automated the process, the better chance illegitimate activity can be detected and resolved in close to real-time, which is likely what will be needed long term if bad actors continue to elude basic blocking techniques.
- To be clear, this is a technique that is for VoIP/SIP specifically. Preferably for end-to-end SIP, but might have use shorter term for some PSTN Gateway to SIP call scenarios as well.

1.7. Certificate Framework and Administration

1.7.1. STIR/SHAKEN are dependent on the use of X.509 certificates for the creation and validation of SIP Identity header described in the IETF standards draft draft-ietf-stir-rfc4474bis”identity header signature.

1.7.2. SHAKEN currently defines the role of Telephone Authority (TA) to support Certificate Authority activities that are specific to the role of trust anchor and root certificate provider.

1.7.3. A more detailed governance role is required to enable the certificate management requirements implemented by the Telephone Authority. This will ensure that

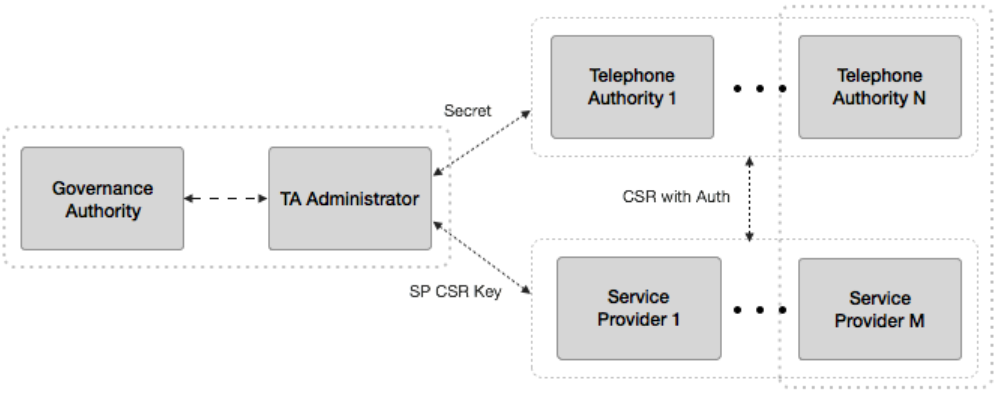
authentication mechanisms are secure and only accessible to authorized users of the telephone network (i.e. Operating Company Number (OCN) owners).

1.7.4. A Telephone Authority, from a process perspective, only deviates from a traditional certificate authority in a few ways:

- Traditional certificate acquisition is a manual process.
- ACME, defined in IETF draft *draft-ietf-acme-acme*, defines a method of providing an automated API for certificate acquisition.
    - We can utilize a secure authentication and authorization framework around ACME Application Programming Interface (API) to provide a straight forward and automated process for both administration and secured usage of Telephone Authorities to create signed certificates by service providers versus potentially more error prone and less secure manual methods.

1.7.5. Proposed Governance and Administrative Framework

- The following diagram represents the logical entities that would be involved in the implementation of a SHAKEN Certificate Framework



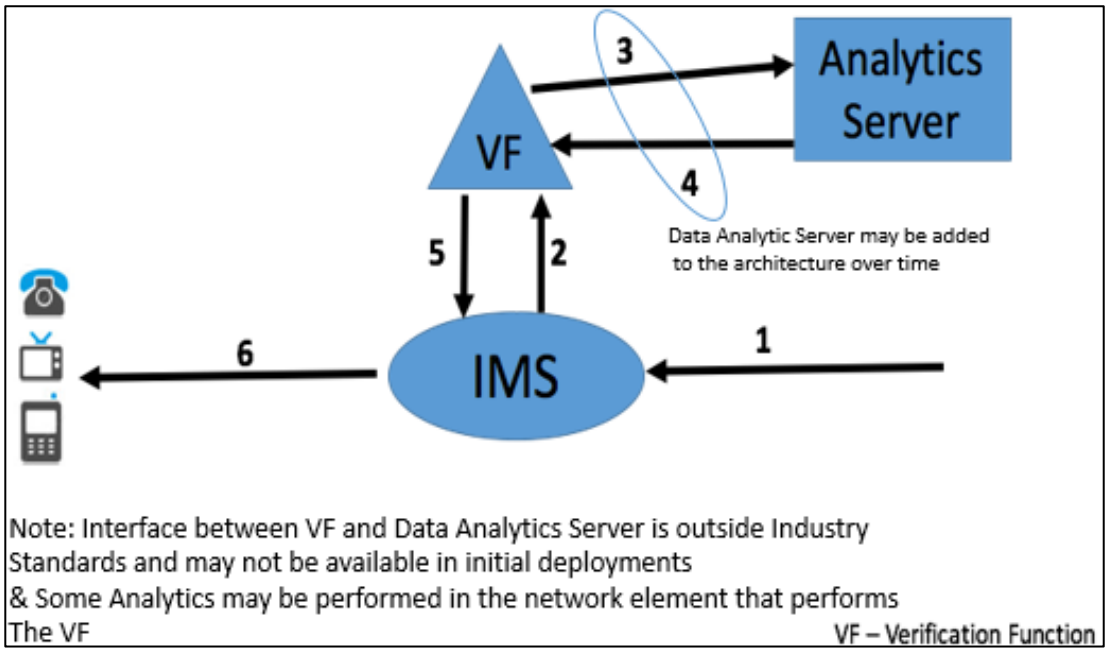
- Governance Authority - this entity would manage, likely tied with identification and potential prosecution of bad actors, the authority for service providers to originate signed calls to the telephone network.
- TA Administrator - this entity would do the manual process of working with service providers to validate they are who they say they are and manage credentials of Telephone Authorities to have a secret key and the Service Providers to do Certificate Signing Requests (CSR) transactions with the Telephone Authorities. They should also have a periodic re-validation and new key issuance, as part of good practice to protect the Telephone Authority services.
    - Note: Governance and Administration are two logical functions but could be supported by a common low administrative overhead organization.
- Telephone Authorities - Can process automated CSR via ACME protocol from Service Providers creating new certificates.

- Service provider - Own and manage a SP certificate key which must be signed by TA.

1.7.6. Proposed framework implementation

- More than one authorized TA would benefit the industry through competition. Verification services will need to explicitly add an authorized TA to their list of acceptable TA root certificates. Each country or jurisdiction should be limited to a "reasonable" number (i.e. likely do not want a proliferation of TAs being established). Looking forward, each country/country code will likely be responsible for approved root TAs and therefore will potentially add significantly to the number of TAs that need to be known by the verification service. This should be considered.

1.8. Signaling-Verification and Analytics Information



1.8.1. Provided the Verification Status and an Analytics Spam Indicator

- Telephone Number Validation Passed

  tel URI parameter in the P-Asserted-Identity or FROM header field in a SIP requests
  P-Asserted-Identity: tel:+14085264000;verstat=TN-Validation-Passed

- Telephone Number Validation Failed
- No Telephone Number Validation
- Future: Same values above for Caller Name (CNAM)

1.8.2. Noted security considerations

- The Verification Function must drop a verification status telephone number Universal Resource/Request Identifier (URI) parameter received in a SIP INVITE signaling request.
- If the terminating User Equipment (UE) does not support the "verification status" parameter value, it must discard the parameter
- The terminating UE will act on the "verification status" parameter value, if the 200 (OK) response to the UE REGISTER includes a Feature-Caps header field, as specified in RFC 6809°[190], with a "+g.3gpp.verstat" header field parameter

1.9. Data Analytics Information

1.9.1. The IETF Draft SIP Call Information Parameters for Labeling Calls provide call information including spam probability, type of call or caller, reason and source of the call. This information is optional and may appear in any combination or order.

1.10. Standards Goals

Completed Short Term Goals:

1.10.1. Accelerated network authentication standards approvals to October from December.

- Internet Engineering Task Force (IETF) has given a last call date of late October for feedback with final approval of October 31, 2016.
- ATIS-SIP Forum letter ballot approval on the SHAKEN framework was accelerated to October 5, 2016 from December providing an approved implementation profile for service providers using STIR.

1.10.2. Submitted requirements change request for handset and display standards to 3GPP.

- Service requirement change requests for signaling from the network to a mobile device was agreed to at the August 3GPP meeting, with approval confirmed at the September meeting.
- Discussion paper, work item, and change request to 3GPP CT1 and CT3 for modifications to 3GPP TS 24.229 and 29.165 for signaling verification information from the network to the device in the call/session setup signaling to be contributed to their October meeting.

1.10.3. Selected solution for Signaling System 7 (SS7) interworking with VoIP authentication.

- The Strike Force has reviewed the potential options, as identified in Section 7 of the ATIS Technical Report on Use of the ISUP Screening Indicator for Conveying Caller ID Authentication Information (“ATIS Technical Report”), to extend authentication and verification interworking through SS7 to TDM/POTS service and has recommended the following:

- Solution 3 in the ATIS Technical Report is the most viable of the solutions as it provides the greatest integrity of the Calling Party Number (CgPN), while being the least impacting to existing customer expectations with respect to delivery of CgPN.
- For solution 3, the successfully verified signed PAI or FROM headers, attesting that the device can use the TN, are interworked into the CgPN with a SI value of "user provided, verified and passed". It differs in that if the PAI or FROM headers are not signed, a "network provided" number (e.g., pseudo number that is unique to each carrier) is populated into the outgoing ISUP CgPN parameter with an indication of "network provided" in the SI field.
- The pseudo number would be unique per carrier for the purpose of traceback and have an associated Calling Name with a value of "UNVERIFIED". This solution does not assume that all subscriptions have Calling Name service. Through consumer education, the pseudo number would be recognized as an unverified number. This is to ensure backward compatibility with earlier generations of caller ID devices that only support numeric ASCII characters. The decision point on whether to proceed with the solution should be made, consistent with the analysis in the ATIS Technical Report, at a time in the future when 50% of VoIP calls are being "fully attested to", taking into account:
  - State of Circuit Switch to IP transition and its trend line
  - Impacts to Government Priority Services
  - Analysis impact of deployed capabilities on Robocalling
    - Authenticated/verification with STIR/SHAKEN
    - DNO
    - Data Analytics
    - Others

1.10.4. Initiated joint lab prototype testing between service providers.

- 3Q 2016: Software added and configuration changes made for provider-to-provider routing via the internet between service providers conducting initial testing.
- 3Q 2016: Initial testing successfully authenticates and validates the basic Identity Header.
- Mid- 3Q 2016: Lab to lab prototype testing within ATIS test bed focus group expanding carrier to carrier interoperability testing.
- 1Q 2017: Expand testing to include SHAKEN certificate framework

Long Term Goals:

1.10.5. December 2016: Complete SHAKEN certificate framework standards based on governance model determined in Strike Force.

1.10.6. April 2017: Checkpoint for IETF work on defining Call-Info call classification and response codes for unwanted calls.

- SIP Call-Info Parameters for Labeling Calls
    - draft-schulzrinne-dispatch-callinfo-spam-00
- A SIP Response Code for Unwanted Calls
    - https://datatracker.ietf.org/doc/draft-schulzrinne-dispatch-status-unwanted/

1.10.7. ATIS-SIP Forum to create best practice on metrics for each carrier to maintain

- Metrics include but not limited to all of the items in the two figures 1.3 and 1.4.
- October 2016: Creation of the best practice Handed off to Susan Miller/Richard Shockey from ATIS/SIP Forum IP NNI Task Force to be addressed in the November 2016 IPNNI meeting.
- Availability of carriers to track their progress against the ATIS/SIP Forum metrics. Beginning at metrics approval. Industry approval of certificate framework. Approval by 1Q17.

1.11. Cost Considerations

Work Group	Cost Impact Areas
Authentication (WG1)	New network upgrades to sign and verify calls; upgrades to supporting operations support systems; certificate management.

Once authentication standards are finalized and vendor capability is developed, carrier network changes will be required in order for calls to be signed by the originating carrier and verified by the terminating carrier. Existing network elements, such as application servers, breakout gateway control functions, session border controllers, and media gateways may require software updates. Surrounding operation support systems used for provisioning and maintaining those elements will also require modifications. Lastly, there will be ongoing costs associated with certificate management and authentication. Companies may need to consider how to recover the costs they incur and they have several options. See Attachment 1 for a description of the cost recovery mechanisms available to the industry.

2. Empowering Consumer Choice

Co-Chairs: Rob Kubik, Samsung / Brad Gaunt, Sprint / Tim Powderly, Apple

Robocall Strike Force members from across the telephony ecosystem came together to provide the end user with a greater degree of identification and control over the types of calls they receive. To address the short term need for call blocking solutions, the group developed a plan to educate consumers on the capabilities existing in the market. To address longer-term needs, this group has agreed to develop information flows, consumer presentation and consumer-directed call disposition control options for standards groups, as well as a plan to deploy resulting solutions. These will give consumers a clearer picture of the type of calls they are receiving, and expand their automatic and manual call handling options.

Consumers today face three problems in availing themselves of robocall protection: low rates of adoption of available solutions, limited availability of solutions, and limited effectiveness of available solutions. A plurality of experts believe that less than 10% of consumers currently are using available call blocking solutions (e.g., whitelist and dynamic blacklist based solutions for TDM, VoIP and wireless technologies).

While most VoIP and wireless customers have access to these solutions many wireline customers do not. And no solution available today is completely effective at blocking spoofed calls without encumbering calls from unknown callers, and blocking product recall notices or other desirable automated calls. Solutions will always have some level of false positives. The Empowering Consumer Choice group's work addresses the first problem by:

- Helping to raise consumer awareness of available robocall defense solutions.
- Encouraging development and increasing effectiveness of new solutions through outreach to developers and through the creation of an improved information framework on which to base more effective information display and call handling solutions.

Consumer Benefit

Created awareness campaigns to educate consumers on existing blocking technologies in the short term and developed an environment where additional capabilities can be developed to facilitate consumer choice.

Section	Task	Estimated Date	Group
Empowering Consumer Choice			
Short Term			
2.3	Created awareness campaigns to educate consumers on existing blocking technologies in the short term and developed an environment where additional capabilities can be developed to facilitate consumer choice.	October 26, 2016	N/A
2.3	Delivered a standardized framework for delivering information from the network to device to empower consumers to make informed call decisions. This framework covers: Call Information flows, Call Disposition Options (including automated Call Disposition), and Feedback Mechanisms from the end user.	October 26, 2016	N/A
Long Term			
2.2.1	Delivery of call validation results based on authentication standards	3Q 2017	ATIS
2.2.1	Develop mechanisms for flexible consumer call control	Current and On Going	CTIA/USTelecom Membership
2.2.1	Each network operator/Original Equipment Manufacturer (OEM) commits to permit a variety of network and/or device control tools.	On Going	CTIA/USTelecom Membership
2.2.2	Implement the capability for customers to feed information back to the service provider.	On Going & Network Dependent	CTIA/USTelecom Membership

2.1 Short Term Goals

2.1.1 Delivered a standardized framework for delivering information from the network to the end user device to empower consumers to make informed call decisions. This framework covers: Call Information flows, Call Disposition Options (including automated Call Disposition), and Feedback Mechanisms from the end user.

2.1.2 Recommended an outreach and education plan to ensure that consumers know of the range of tools available today to combat unwanted robocalls, provide continued consumer education so they learn of the improvements to existing tools, as well as the new approaches that will flow from the work of the Strike Force.

2.2 Long Term Goals

2.2.1 Successfully drive adoption of standardized framework for delivering information from the network to device to empower consumers to make informed call decisions.

- Delivery of standards based on authentication standards.
- Develop mechanisms for flexible consumer call control
- Each network operator/Original Equipment Manufacturer (OEM) commits to permit a variety of network and/or device control tools.
- Implement the capability for customers to feed information back to the service provider.

2.3 Outreach Plan

2.3.1 Consumer outreach is a key component of the Strike Force's program. We must ensure that consumers know of the range of tools available today to combat unwanted robocalls, and that we have a structure in place to ensure that consumers learn of the improvements to existing tools, as well as the new approaches that will flow from the work of the Strike Force. In doing so, we designed a consumer outreach plan that (1) allows consumers to seek information that is most relevant to their technologies of choice; (2) scales as new companies and organizations join our efforts; (3) makes it easier for consumers to find relevant information; and (4) does so without creating a burdensome or unsustainable centralized process given the wide array of entities with information relevant to consumer needs. Consumer education and adoption of existing device blacklist capabilities can immediately address a substantial percentage of unwanted robocalls.

2.3.2 Furthermore, third-party solution developers as well as network operators play a role in consumers' ability to better control unwanted robocalls. Therefore, the Strike Force's outreach plan includes efforts to reach out to the community of innovative solution developers to (1) encourage accelerated development efforts; (2) effectively communicate technical changes to networks and devices that will allow more effective applications; and (3) permit Strike Force members to integrate new solutions or even new classes of solutions to consumers as part of our overall outreach effort.

2.3.3 To advance these goals, this section of the Report first describes the consumer outreach commitments and programs of individual organizations communicating with wireline consumers, wireless consumers, and the solution development community. Next, it describes a new multi-sector effort to making it easier for consumers and applications developers to access the information they need, when they need it, for the technology of their choice—and to ensure a mechanism is in place to efficiently update consumers and applications developers of the advances stemming from the work of this Strike Force.

2.3.4 Intensifying Consumer Outreach Commitments by Sector.

- The first step of the Strike Force's consumer outreach plan is for organizations representing each of the major telecommunications industry sectors to intensify outreach to consumers of their technologies. This section describes the efforts planned for wireline consumers, wireless consumers, and VoIP consumers.
    - Outreach to wireline and VoIP consumers will be provided by USTelecom, NTCA-The Rural Broadband Association and NCTA – Internet and Television Association.
    - To arm consumers with information they can use to block or filter unwanted calls, the VON Coalition will provide links on its website, www.von.org, to its members' resources describing how to stop robocalls to VoIP services.
    - Outreach to wireless consumers will be provided by CTIA.

2.3.5 Launching a New Central Information Resource for All Consumers.

- In addition to the acceleration in the outreach conducted by the above organizations, the Strike Force recommends initiating a new multi-sector effort to making it easier for consumers and applications developers to find the information and tools appropriate to their individual needs.
- The FCC and Strike Force members, and the industry associations jointly agree to: (1) maintain a central site hosted by the FCC where all consumers can learn about the tools available, learn how to protect themselves, and find the resources tailored to their needs from the companies, trade associations, and consumer organizations of their choice; (2) organize a website launch on 10/26/16 during which the FCC and the Strike Force can announce the new site, make key individuals available for media outlets, and focus consumer attention; and (3) because of the central role that third-party applications will play in allowing consumers to tailor robocalls control to their individual needs, launch an aggressive new outreach program to the developer community to spur a more powerful next generation of applications.

2.3.6 Robocall Control Web Portal.

- Strike Force members will work with the FCC to develop, launch, and maintain a new one-stop website as a central resource for consumers. This site will consolidate consumer and developer robocall control resources across wireline, wireless, and VoIP technologies. Importantly, to avoid bureaucracy and delay and to allow innovation, the FCC should design the site to allow consumers to quickly and easily access the information sources they need through links to external

websites, rather than forcing the wide array of companies, trade associations, and consumer groups to submit content and resources for publication by the FCC.

- Several of the leading organizations with robocall control resources have already agreed to participate. CTIA, USTelecom, The Internet and Television Association (NCTA), and The Application Association (ACT) have each committed to this plan. To maintain currency of resources, reduce time delays, and allow ongoing supervision by subject matter experts within different contexts, participating organizations will host substantive materials, reached by links from the main page organized by technology or type. For example, CTIA has volunteered to host wireless resources, USTelecom has volunteered to host wireline resources, NCTA has volunteered to host cable telephone resources, and ACT has volunteered to host third-party developer resources.

2.3.7 Launch Event

- To maximize public awareness of the consumer and developer resources described above, the Strike Force members will meet October 26th at the FCC to launch the FCC robocall blocking consumer resource site.

2.3.8 Promoting a New Generation of Robocall Control Apps.

- Third-party applications as well as network operators play a critical role in empowering consumers to control robocalls. The Strike Force will therefore work with ACT to support the development of more powerful apps to increase consumer control over robocalls. Specifically, ACT's work will include three key deliverables:

    - A public-facing website that provides technical information and recommendations for current and potential robocall control app developers, including technical updates related to changes to information provided by networks on call spoofing or signaling systems that applications can harness. The website will also provide app developers information on privacy and privacy policy best practices. ACT will design this information to make it easy for app developers to capitalize on the approaches developed by the Strike Force and to create innovative new solutions.
    - Targeted outreach to ACT members, including more than 5,000 app companies and IT firms from across the mobile economy. ACT will use its range of communication mechanisms, including online tools, newsletters, reports, and white papers to educate members about opportunities to develop robocall control apps.
    - An online workshop for developers offering both real-time participation and access through ACT's archives. The workshop will work to catalyze the creation of new apps by helping developers quickly get up to speed on the technical and policy considerations behind robocall control apps.

2.4 Framework for the End User

To address longer-term needs, this group has agreed to develop information flows, consumer presentation and consumer-directed call disposition control options for standards groups, as well as a plan to deploy resulting solutions. These will give consumers a clearer picture of the type of calls they are receiving, and expand their automatic and manual call handling options.

2.4.1 **Assumptions**

- Changes requiring switch or feature development may not be feasible, especially for equipment that is manufacturer discontinued. This includes changes in call processing, feature controls and feature operations, or reuse of existing CLASS features.
- Services requiring new Vertical Service Codes (VSC) will also depend on the carrier's ability to implement the feature requirements in the absence of manufacturer support.
- New service codes could be in the extended, if determined feasible by standards organizations, 3-digit code [*2X] range.
- Each VoIP call will ideally supply the end user with the Calling Party Name (CNAM), Calling Party number, an authentication indicator, and the call category. It will depend on the end device to be able to display what is contained in the field.
- In addition, providers that are transitioning to IP networks in whole or in part, or are planning to start in three years, should not be expected to spend resources on the legacy platforms so as to enable the acceleration of the transition to IP.

2.4.2 Call Information Fields:

Varying vendor's user interfaces may utilize some or all of the following fields to enable consumer choices:

Calling Party Name

- Wireline
    - For wireline consumers, names are retrieved based on the calling number. If the number is spoofed or unspecified, the name retrieved will also be for the spoofed number. Improving the integrity of the calling number improves the quality of the displayed name.
    - A potential option for providing wireline consumers with information they can use to mitigate robocalls is for the terminating carrier to add an indicator (such as an asterisk) to the calling party information transmitted with calls flagged by an analytics engine as potentially unwanted.
    - Another option is to implement a network level solution that deploys analytics and crowd-sourced feedback to create a dynamic list accessible to all subscribers with differing treatment options as chosen by the individual consumer – blocking, allowing, or message (voice mail). The larger benefit is that the decision to route or block the call can be made at the routing point of the provider's central office or node without additional hardware and may therefore require minimal investment by individual carriers.
    - Furthermore, the value of the CNAM service deteriorates when more and more service providers do not provide access to their name data/databases.

All carriers should consider making names available for retrieval as part of the caller identity ecosystem to the extent authorized by consumers.

- Having recognized the importance of the calling number's validity, the Strike Force recommends that the industry take measures for preserving the integrity of the name data.

- VoIP and Wireless
  - The enhanced CNAM (eCNAM) service was introduced to improve the consumer experience with the popular CNAM services. eCNAM, however, was designed for the VoIP and wireless customers. The goal was to make available a name longer than 15 characters (a limitation of the legacy network and Customer Premise Equipment (CPE) and to provide additional information about the caller. The additional information is subject to the caller's consent. Consumers' requests for this additional information increased with the plague of robocalling. Armed with "more" information, consumers feel empowered. Businesses that are calling with no intent to scam or harm the consumer are eager to deliver more information about themselves (address, type of business, BBB standing, etc.) VoIP and wireless devices are more capable of handling this additional information. eCNAM consolidates the name and the metadata in one service.

Calling Party Number

- Wireline/VoIP
  - On calls originating from wireline consumers, the calling party number is supplied in the signaling of the call. The terminating wireline switch uses this information to provide the calling number to the consumer's Caller ID capable CPE.
    - Innovation may be used to develop a designated "pseudo number", unique to each carrier, could replace the display of calling numbers that are not verified. A matching name (for customers that subscribe to CNAM) could be displayed as "unverified."

Authentication Indicator

- Wireline
  - Caller ID customers are limited to the capabilities of the TDM (Time Division Multiplex) services and the traditional caller ID devices. The display provides a 10-digit telephone number and a 15-character name. Since SHAKEN (Signature-based Handling of Asserted information using toKENs) verification does not take place in TDM, it may be possible to use analytics, where available, that convey an "indicator" of a verified number in the leading or trailing character of the Name display.

- Within the constraints of TDM services, this idea offers more information to the wireline user. However, industry groups, such as ATIS and service providers need to consider/study:
  - The impacts of introducing that change for every CNAM customer on every call.
  - The effectiveness of educating consumers on the meaning of the new character introduced (e.g., an asterisk).
  - If there are limitations to the type of characters that may be used.

- VoIP
  - VoIP networks are capable of implementing an authentication indicator to display on capable CPE
  - VoIP Interoperability with wireline networks using the SS7 Calling Party Number Screening indicator may be used to provide interworking of an indicator of authentication.
  - However, some currently deployed gateways may not support this interworking. Additionally it is unknown if all wireline circuit switches are capable of the Calling Party Number Screening standard (ATIS-1000625) or if an indicator set as untrusted will maintain the calling party number and its screening indicator through the interworking process. Standards Modifications are needed.

Call Categories

- The following Call Categories are recommended for inclusion in the standards and signaling process. These categories are intended to be consumed primarily by analytics applications. However, the analytics may present information based on these categories to the consumer to assist in their call control and management.
  - Telemarketing – Calls originated in order to induce the purchase of a product or service to the end user
  - Survey – Call originated in order to collect data / opinions from an end user
  - Political – Call originated with intent to pass a political message to the end user
  - Charities / Non-profit – Call originated from a non-profit company with intent to inform or solicit information or money from the end user
  - Informational – Call originated from an entity to inform called party of an already established business relationship transaction such as package delivery, appointment reminder, order confirmation, conferencing, etc.
  - Emergency/ Public Service – Call originated from a supplier that is delivering an emergency or public service type call

- Collection – Call originated from a company with the intent to collect outstanding funds from the end user
- Healthcare – Call originated from a company with intent to provide health care information to the end user such as doctors, nurses, insurance companies
- Basic/ Personal – Call originated from a party that just wants to speak personally to the end user (Grandma calling Grandkid)
- Trusted Entity – Call was originated by a trusted entity whose calling patterns such as conferencing or messaging cannot be covered by the listed calling categories but they are an established trusted source
- Spoofing – Possible spoofed caller ID
- Suspected fraudulent calls – Suspected Fraudulent call

- Wireline
  - It may be possible for industry groups and service providers to consider the feasibility and impacts of bridging audio announcements that voice the category information to the wireline consumers as soon as they answer, and prior to being connected to calling party; i.e., delay completing the incoming call for 20-30 seconds while providing an announcement.
  - Alternatively, where available, Distinctive Ringing could be applied to incoming calls that are deemed "unverified" by the service provider's analytics.
  - Given that most of the above metadata are not signaled in legacy networks, the terminating service provider has a potential to launch queries to databases that contain the same or similar information. Such queries from the terminating end could bypass the limitations of legacy signaling and still bring some value of analytics to the wireline consumer.
  - Other solutions could include, where available, the use of simultaneous ring where a service (such as Nomorobo) is enabled at a secondary location to screen the call. If the caller information is legitimate, the call goes through to the customer. Otherwise, the caller is disconnected, and the customer's phone only rings once then stops. Not all wireline circuit switches are capable of simultaneous ring.
  - Consumers could customize their robocalling treatment preferences for each of the above "categories" via a yet to be developed web interface or with capable devices. Providers of solutions for unwanted calls would design the solution based on those preferences.

- VoIP
  - Industry should adopt the list above in the VoIP environment as best practice.

- It can be potentially used for analytics, call labeling, and provide end users with distinctive rings.

Risk Score

- Call Control Providers may use industry best practices surrounding the risk scoring of a number, when applicable, to help the customer make an informed decision about the call. Companies may utilize their own scoring mechanism to rank a call's risk.
- VoIP
  - The following link proposes a set of Call-Info parameters that allow the carrier or other UE-trusted SIP entity in the path to indicate the spam probability, type of call and other related information that will allow the UE and user to make better call handling decisions:

    https://datatracker.ietf.org/doc/draft-schulzrinne-dispatch-callinfo-spam/

2.4.3 Call Disposition: Solutions could provide flexible options or call dispositions that reflect consumer's needs. Examples include:

Prior to accepting call: Defer to voicemail, Request for voice identification, Decline

- Wireline
  - Due to constraints of TDM technology, wireline customers are not able to "redirect/reject" incoming calls before answering. However, some services exist today in some networks that use call features that may allow the request of voice identification before completing the call. This helps reject calls with pre-recorded messages, which can also be viewed as the equivalent of requesting voice identification.

Post Call Treatment: Block future call

- Wireline / VoIP
  - Following the call, vertical service codes (such as *57) are available for the consumer to report harassment and requires law enforcement involvement to obtain records.
  - Further investigation is needed (by ATIS and service providers) to determine if the use of the Call Trace *57 could be augmented to report suspicious robocalls. The reported numbers could be added to the service provider's analytics and/or black lists.
  - For VoIP the reported numbers could be added to the service provider's analytics and/or black lists via a portal.

2.4.4 Feedback to Solution Provider:

- Wireline/VoIP

- Starcode: Further investigation is needed (by ATIS and service providers) to determine if the use of the Call Trace *57 could be augmented to report suspicious robocalls.
- Web portal: Each service provider may consider educating their consumers to report suspicious robocalls through designated web portal(s).

- Wireless
  - Report (spam or not spam)
  - As an example, the following link defines a new proposed status code (666) that users can use to mark unwanted calls, either as a response code to an INVITE or in a Reason header in a BYE response:

    https://datatracker.ietf.org/doc/draft-schulzrinne-dispatch-status-unwanted/
  - Alternatively, API-based mechanisms can support post call spam reports.

2.4.5 Automated Disposition: Solutions could provide flexible options or call dispositions that reflect consumer's needs. Examples include:

Decline or Send to Voicemail by:

- Specified number
- Call Category
- Risk Factor
- Authenticated Status
- Pre-defined or solution managed block list

Call disposition can occur in either network and/or device:

- Wireline
  - Both network-based and device-based solutions may be available to wireline consumers depending on the network. It should be noted, however, that most of these services strictly compare the incoming Calling Number to the entries on the list. This means that both a spoofed call and legitimate call from the same Calling Number will be handled identically.
  - Network-provided SCA and SCR

    Customers may have access to Selective Call Acceptance (SCA) and Selective Call Rejection (SCR) lists from their service providers today. The lists allow the consumer to specify and update a limited amount of TNs on each list. While some wireline consumers may find the interface for managing the lists cumbersome, these features already exist for consumers to utilize. However, augmenting the size of the lists is not possible for wireline customers due to switch memory capacity – given most Class 5 switches are manufacturer- discontinued. For VoIP customers, the list capacity limitation may not exist and the user interface may be less cumbersome.

  - SCA (Personalized White List): Incoming call attempts from calling TNs on the list will be completed. Incoming call attempts from Calling TNs that cannot be identified or have not been indicated in the SCA list will be prevented from terminating to the customer's line. Instead, these callers could be connected to an announcement stating that their call is not presently being accepted by the customer. SCA can be effective in blocking unwanted calls to highly vulnerable individuals or other people who should only receive calls from a very small quantity (typically fewer than 10) of phone numbers.
  - SCA implemented with a 'divert all callers not on the acceptance list' policy can reduce annoyance, but impedes the ease and openness of wanted communications from unanticipated phone numbers.
  - SCR (Personalized Black List): Incoming call attempts from calling TNs on the list will be connected to an announcement stating that his/her call is not presently being accepted by the customer. Call attempts from calling TNs that do not match entries on the SCR list are given standard terminating treatment. SCR in itself is effective against only persistent harassment from a small and well known set of phone numbers; it is largely ineffective against the current robocall threat originating from a large and changing set of possibly spoofed phone numbers.

- Telephone Accessory Solutions Features:
  - **Device-Based Blacklist/Whitelist:** Some devices (i.e., in-home accessory boxes and high-end wireline phones) employ personalized blacklists and whitelists to help manage unwanted calls. These devices may suppress or offer a distinctive ringing experience for unwanted calls. They may also offer an alternative call handling, such as routing to a built-in answering machine.
  - **Challenge Mechanism:** A personal blacklist and whitelist (like SCA's) combined with a challenge mechanism (e.g., an audio challenge "no soliciting, press 1 if this is a non-commercial call to continue" to callers not on the list) for callers that are NOT on the whitelist can be an effective defense. Calls that fail the challenge may be handled with an appropriate action other than ringing. This type of solution is available to wireline consumers today in various appliances. However it impedes the ease and openness of communications from unanticipated phone numbers.
  - **Dynamic Blacklist**: Some accessory solutions feature an externally-managed blacklist of phone numbers known to originate unwanted calls as well as "crowd-sourced" unwanted call feedback to the blacklist manager.
- VoIP
  - For VoIP customers, the capacity limitations may not exist.

- Customers today have the ability to manage their settings via web portals and mobile apps to control call disposition

2.5 Summary of Action Items

2.5.1 Wireline Summary

Despite the technical limitations of TDM technology compared to wireless and VoIP, legacy wireline networks can, in many cases do, employ a number of tools that improve the wireline consumers' ability to deal with unwanted calls.

In particular, calling number validation, described in Section 1, will improve the integrity of the services that rely on the calling number, such as Calling Name, Selective Call Acceptance and Selective Call Rejection or Call Trace.

Most of the unwanted calls reach wireline subscribers through VoIP gateways. VoIP gateways may be augmented to implement calling number validation, do-not-originate policies and call filtering to reduce the number of unwanted calls that reach wireline subscribers.

In addition, there are a number of possible capabilities of features of the TDM network that could be reused. In particular, simultaneous ringing sends the call first to a screening service. If the call is legitimate, the call rings through to the customer. Otherwise, the unwanted caller is disconnected, and the customer's phone only rings once.

Reporting robocalls helps in improving call filters and tracking down illegal robocallers. For wireline customers, reporting could be accomplished by dialing a Vertical Service Code following the suspicious call. Carriers may also provide consumers with website to report illegal robocall complaints. (www.fcc.gov/robocalls)

Where available, utilizing network resources such as distinctive rings and audio announcements could prove useful in relaying the verification results to the consumer in a manner compatible with existing technology. However, it should be noted that some of the proposed solutions will require varying levels of modifications to the switches and the service logic. That presents an implementation challenge where circuit switch manufacturers have discontinued production and support of these switches. Fortunately, some wireline networks are hybrids, consisting of modern VoIP switches serving analog loops.

Some of the solutions, such as call status announcements, will also require exceptions or relief from current FCC Rural Call Completion rules on post-dial delay, provided the called party consents to that treatment.

Lastly, the success of the approaches described in this report will depend, to a large extent on the success of the outreach programs that educate consumers on the nature and risk associated with some robocalls, and the different tools available to combat them.

2.5.2 Wireline Action Items

- It is recommended that the entities listed in this section (industry bodies, FCC, etc.) address the action items with an expectation that they work towards a goal of 3-4Q17.
- ATIS Committees such as INC, PTSC, NGIIF:
    - Investigate the feasibility of using *XX codes to report unwanted robocalls. Could existing codes be reused, and how could that be achieved with minimal changes to existing legacy infrastructure? Does this idea warrant standards or

industry best practices? Should a new Vertical Service Code be considered? ATIS has agreed to progress this effort and investigate the feasibility of *XX codes.

- If announcements are played (to inform the customer of the risk status of the call) BEFORE connecting the incoming call, then some delay is imminent (~15-20 sec). That will require relief from the FCC on current rules regarding post-dial delay.
- Service providers and switch equipment community: investigate the feasibility of modifying the traditional capabilities or services, such as CNAM string to include a verification indicator prior to delivery to the customer, or new *XX codes, or delayed answer with announcements, as discussed above.

2.5.3 **VoIP Summary**

Constructing the best practices was defined within this document as it may take some time for the industry to adopt these practices and end device manufactures to embrace them.

Increased reliability and availability of the calling number in order for call management features (CNAM, selective call rejection or acceptance and call trace) to operate properly.

Enabling/reusing *XX codes to allow consumers to report suspicious calls and also leveraging a web portal to manage consumer selections.

2.5.4 **VoIP Action Items**

- The terminating service provider and analytics providers to consider obtaining information on the calling number and other attributes of the call the pass on to the consumer.
- Third-party applications and APIs today play a central role in the wireless context, providing consumers with a range of robocall-control options.
- Standards Activities:
    - Network-to-device signaling standard for indicating likely nature and spam probability of call (IETF) (2Q-3Q17)
    - Device-to-network call signaling (SIP) response code for indicating call was unwanted (IETF) (2Q-3Q17)

2.5.5 **Wireless Action Items**

- Successful handoff to CTIA membership of the framework guidelines for delivery of information from the network, for purposes of continued support of the framework recognizing ongoing work in standards development organizations, coordination with relevant industry groups (e.g. USTelecom).
- Because third-party applications and APIs today play a central role in the wireless context, providing consumers with a range of robocall-control options, coordinate deliverables with ACT — The App Association, for integration into its new program, so the next generation of applications account for the information flows spurred by the Strike Force.
- Standards Development Activities:
    - Network-to-device signaling standard for indicating that calling party number has been validated (3GPP) (submitted 4Q16) (see Section 1.10.2)

2.6 Cost Considerations

Work Group	Cost Impact Areas
Empowering Consumer Choice (WG2)	Feature development to pass information to end user devices; risk scoring to help customers make informed choices; call disposition options that reflect consumer's needs; feedback to solution providers.

Delivering information from the network to a device to empower consumers to make informed call decisions will require, where possible, feature development. While the ability to deliver new information to legacy systems will be limited by existing capabilities each VoIP call will ideally supply the end user with the Calling Party Name, Calling Party number, and an authentication indicator. This will also depend on the ability of the end device to display what is contained in the field. Call control providers may also invest in analytics and use industry best practices to determine the risk scoring of a number, and call category to help the customer make an informed decision about the call. Feedback to solution providers such as star codes, web portals, and spam buttons will also require additional investments. Companies may need to consider how to recover the costs and they have several options. See Attachment 1 for a description of the cost recovery mechanisms available to the industry.

3. Detection, Assessment, Traceback, and Mitigation

Co-Chairs: Jim Calme, Nokia / Adam Panagia, AT&T

This group investigated various methods of detection and avoidance to stop unwanted calls from reaching customers by blocking at various network levels. This group has initiated a trial to block known numbers that should never originate traffic. The results of this trial will help determine the viability and effectiveness of a Do Not Originate list of numbers to be blocked network wide in the future.

Consumer Benefit

Today, vulnerabilities in the Publicly Switched Telephone Network are being exploited by bad actors to harm consumers. Strike Force members have established industry guidelines to enhance detection, traceback, and blocking of malicious traffic.

Section	Task	Estimated Date	Group
Detection, Assessment, Traceback, and Mitigation			
Short Term			
Detection, Assessment, & Mitigation (Blocking)			
3.1.1	Documented and shared best practices regarding identification of robocalls.	October 7, 2016	N/A
Traceback			
3.1.2	Improved and accelerated robocall traceback.	On Going	USTelecom
Do Not Originate			
3.1.3	Defined "small" set of well-known numbers that are used for inbound only calls	September 15, 2016	N/A
3.1.4	Created cross industry repository of identified Do Not Originate numbers.	October 7, 2016	N/A
3.1.5	Initiated a trial Do Not Originate on a small set of numbers to gauge scammer behavior.	October 7, 2016	N/A
Long Term			
3.2.1	Actively recruit companies to the Industry Traceback Group supported the US Telecom Association (USTA).	On Going	USTelecom
3.2.2	Create a process for regulators and enforcement bureaus to tap into the Industry Trace Back Group to expedite traceback requests.	3Q 2017	USTelecom
3.2.3	Measure the success of the Do Not Originate trial.	January 31, 2017	USTelecom

3.1. Short Term Goals

Detection, Assessment, & Mitigation (Blocking)

3.1.1. Documented and shared best practices regarding identification of robocalls

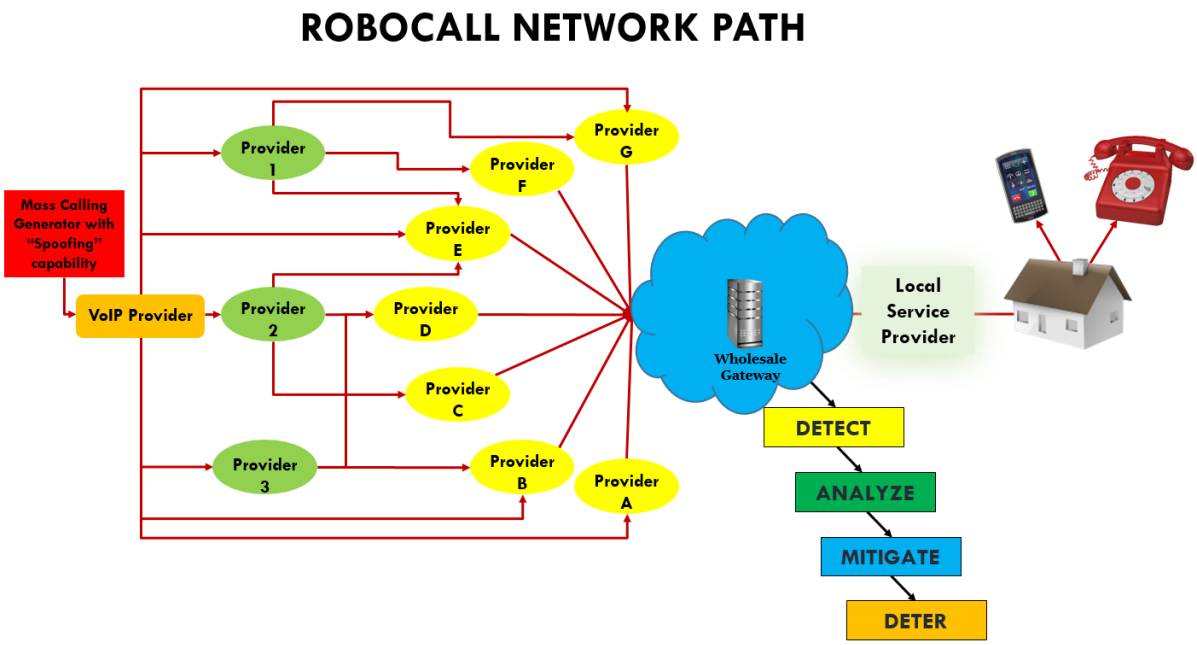
- Discussed best practices on thresholds, techniques, and report format for detecting and blocking large volumes of robocalls on a daily basis.
- Discussed common entry points of bad traffic to the network. Estimated 90+% of robocalls enter the Public Switched Telephone Network (PSTN) through the wholesale VoIP gateways.
    - Best Practices for service providers' detection of robocalls include the use of various confidential detection elements.
    - Carriers using analytics mentioned in the best practices have estimated an average of 67 million blocked calls in September.
        - As an example of the potential of metrics like the above, AT&T has developed analytics to detect robocalling events and has blocked 51% more robocalling since the start of the Strike Force.
    - Defining a single industry-wide profile for the identification of robocalls is not practical due to the differences in the nature of traffic carried, the amount of the traffic, etc.
        - Fraudsters' tactics morph quickly with every countermeasure deployed. Each company will need to constantly define their own robocall profile based on the type of traffic crossing their network, capacity to investigate alleged fraud, and other factors.

Traceback

3.1.2. Improved and accelerated robocall traceback

- Past traceback methodology was manually intensive and time consuming.

- Prior to the industry traceback group, carriers were uncertain of the legal footing of sharing information.
- The work from the Regulatory/Root Cause Removal team has cleared the way for a more cooperative sharing environment amongst carriers.
- The Industry Traceback Group has created an Intransigent Letter to accelerate cooperation and reduce resistance to investigative efforts as the traceback moves upstream.



Do Not Originate

3.1.3. Defined "small" set of well-known, high profile numbers that are used for inbound only calls.

- One carrier examined two years of blocking history and found a robocall number associated with IRS scams is still frequently attempting to reach consumers despite being blocked.
    - Blocked call attempts over 90 day period (July-September 2016): 1.4 million.
    - The data suggests that although one carrier blocked a robocall number associated with IRS scams, the scammers will continue to send traffic because calls will route to another carrier network where blocks are not in place. The entire industry needs to participate for the Do Not Originate blocking effort to be effective.

3.1.4. Created cross industry repository of identified Do Not Originate numbers.

- All participants of the Strike Force have access to the shared list of numbers that should not be originated and can add more for review.

3.1.5. Initiated a Do Not Originate trial on a small set of numbers to gauge scammer behavior and reaction to Strike Force countermeasures.

- The IRS conveyed a 90% reduction in IRS scam call complaints in the last two months, with the largest drop off coinciding with the DNO trial, from a high of 43,000 complaints in late August to only 3,700 complaints in mid-October.
- Permission to block these numbers has been explicitly given by the Assistant Inspector General for Investigations – Threat, Agent Safety and Sensitive Investigations Directorate of the Department of the Treasury.
- The initial results of the Do Not Originate trial has been very optimistic. One Strike Force member noted a dramatic reduction in numbers associated with the IRS scam crossing their network from 8,000 per day to 1,000 since the Strike Force initiated the trial.
- While these statistics are a positive step, further analysis of the Do Not Originate trial findings will examine long term effectiveness as bad actors react and evolve to the Strike Force's efforts.
    - We anticipate that success in blocking the high profile, official numbers will push the bad actors to randomly spoof numbers to continue their scams. If the scammers resort to spoofing legitimate/alternative numbers we cannot block, carriers' course of action will be to aggressively perform traceback and execute root cause removal through actions including enforcement.
    - While adding every number used by scammers to a centralized Do Not Originate database may not be feasible, there is victory in removing the authority gained by spoofing specific numbers customers recognize.

3.2. Long Term Goals

3.2.1. Actively recruit companies in the telecommunication ecosystem to the Industry Traceback Group supported by the USTelecom. The expanded group will:

- Conduct regular, ongoing conversations between regulators, enforcement bureaus and the Industry Trace Back Group to share threat intelligence related to robocalling and call ID spoofing with the goal of expediting traceback requests and reducing the number of legal demands.
- Utilize the SIP header developed by the Authentication work group when implementation is complete in 2018. This will be employed by the Industry Trackback Group to accelerate trackbacks directly to the source carrier of bad traffic.
- Explore ability to ramp up resources and expand coverage hours for personnel responsible for responding to Industry Traceback Group requests.
- Increase participation in the next year to make tracebacks faster, more successful, and identify the abusive robocalling source. Continue recruitment of companies for the USTelecom Industry Traceback Group. Double the participants from 11 to 22 by July 31st, 2017.

3.2.2. Continually enhance industry best practices for traceback

- Incorporated Strike Force carrier members in the Industry Traceback Group. These members are encouraged to participate in traceback events through the Industry Traceback Group.
    - An example of a best practices by Industry Traceback Group members is the Prompt Response clause. This clause confirms member's agreement to rapidly respond to traceback efforts.
        - At a minimum an Industry Traceback Group member investigating Suspicious Traffic originating on, or transiting through its network should provide 1) updates on the status of any investigation into Suspicious Traffic, 2) as-required updates on substantive developments into any investigation into Suspicious Traffic; and 3) resolution of the Suspicious Traffic investigation.
- Expand upon traceback tracking metrics and improve information sharing among the USTelecom Industry Traceback Group. Beginning 10/26 and ongoing.
- USTelecom to provide a bi-annual briefing on traceback progress to the FCC.

3.2.3. Measure the success of the Do Not Originate trial

- Examine the behavior of fraudsters and how they attempt to push traffic through carrier networks after the network blocks have been in effect.
- If determined to be viable, evolve Do Not Originate to larger number data set.
    - Other widely spoofed official numbers could be requested to be added to the Do Not Originate list by the carriers' customer.
    - Determine process for how a telephone number gets added/removed from Do Not Originate list.
- USTelecom to complete report on Do Not Originate including recommendations on future path of Do Not Originate. Completion by 1Q17 with a readout to the FCC.

3.3. Cost Considerations

Work Group	Cost Impact Areas
Detection, Assessment, Traceback, and Mitigation	Big data analytics and tools for identifying robocalls; scalable blocking capabilities; improved and accelerated robocall traceback; "Do Not Originate" solution

Identification of robocalls will require investment in big data analytics and tools. While all networks likely have limited blocking capabilities, additional investment will likely be required for more effective and scalable network blocking capabilities. Improving the cycle time and increasing the number of traceback events will require new capabilities, processes and resources. While the Strike Force Do Not Originate trial will only require limited investment, any expanded solution will require investment in number collection and validation capabilities, repositories, and

interfaces for distributing blocked number information to carriers for blocking treatment. Companies may need to consider how to recover the costs and they have several options. See Attachment 1 for a description of the cost recovery mechanisms available to the industry.

4. Regulatory Support/Root Cause Removal

Co-Chairs: Scott Seab, Level 3 / Chris Oatway, Verizon / Linda Vandeloop, AT&T

This group has supported the Robocall Strike Force's technical working groups by giving guidance about key terminology and the legal landscape, and by helping to remove regulatory roadblocks. They also have developed recommendations for actions the FCC can take to support industry efforts to trace back and to block illegal robocalls.

Consumer Benefit

It is in the public's best interest for government and industry to collaborate on the robocall problem. Government can ensure that industry has the flexibility to use robust tools to address illegal traffic on its own and industry can facilitate government efforts to investigate and shut down the illegal robocall operations that are the root cause of the problem.

Section	Task	Estimated Date	Group
Regulation/Root Cause Removal			
Short Term			
4.1.1	Provided Guidance on regulatory rules to facilitate identifying and stopping robocalls from reaching the consumer.	October 26, 2016	N/A
4.1.2	Obtained FCC clarification that carriers may block calls when instructed by the subscriber of a spoofed number. The FCC provided that clarification on September 30th.	October 26, 2016	N/A
4.1.2	Drafted request for FCC clarification that carriers may block calls that determined to be illegal.	October 26, 2016	N/A
4.1.2	Drafted request for clarification that carriers can share information on retail and wholesale customers to investigate and trace back illegal Robocall campaigns to the source.	October 26, 2016	N/A
4.1.2	Developed proposed safe harbor for carriers acting in good faith from enforcement actions for inadvertently blocking a legitimate call.	October 26, 2016	N/A
4.1.2	Developed a process to maintain a contact list for Robocall related subpoenas.	October 26, 2016	N/A
Long Term			
4.1.3	Work to shorten the cycle time from identification to stopping the illegal activity.	On-going	USTelecom
4.1.4	USTA will oversee the review and discussion of a proposed Transferable Cease and Desist with a safe harbor for cooperating carriers	1Q 2017	USTelecom

4.1. Provided Guidance on regulatory rules to facilitate identifying and stopping robocalls from reaching the consumer

- Established criteria for initiating tracebacks of suspicious traffic.
- Guidance on when blocking is acceptable and proposed a safe harbor for cooperating entities.

4.2. Recommendations to FCC on actions for government

- Obtained FCC clarification that carriers may block calls when instructed by the subscriber of a spoofed number. The FCC provided that clarification on September 30th.
- Drafted request for FCC clarification that carriers may block calls after following industry best practices for due diligence investigations.
- Drafted request for clarification that carriers can share information on retail and wholesale customers to investigate and trace back suspected illegal robocall campaigns to the source.
- Developed proposed safe harbor for entities acting in good faith from enforcement actions for inadvertently blocking a legitimate call.
- Proposed an amendment to 47 C. F. R. section 64.2105 to state that calls blocked to protect consumers from receiving illegal robocalls will not be considered when evaluating the long distance call completion rates.

4.3. Work with Enforcement to shorten the cycle time from identification to stopping the illegal activity

- Developed a process to maintain a contact list for robocall related subpoenas. The list will be maintained by ATIS and can be accessed by enforcement agencies. The list will be updated by ATIS members and the industry trusted carrier traceback group.

4.4. Handoff to USTelecom to continue the longer term policy development

- Resolution of regulatory issues identified during the strike force and any new issues identified during traceback requests. Beginning October 26, 2016 and on-going.
- Refine the process to expedite traceback requests and reduce legal demands including review of a proposed transferable cease and desist order or subpoena. Completion by 3Q17.
- USTelecom, with participating service providers, many of whom are Strike Force members, will review whether there is a need for regulatory action concerning the fact that some of the solutions, such as call status announcements, may also require exceptions or relief from current FCC Rural Call Completion rules on post-dial delay, provided the called party consents to that treatment.
- USTelecom will review impacts on CALEA. The changes to the delivery of Meta data (Number, eCNAM, CNAM, +g.3gpp.verstat header field parameters validating such Meta data) and blocking of calls may impact call intercept information collected and supported under CALEA. Those issues should be discussed with Law Enforcement Agencies (LEA) to assess any impacts to them and safe harbor considerations. This may induce new costs into CALEA delivery mechanisms that are not currently supported.

5. Cost Considerations

The Robocall Strike Force has reinforced that effective mitigation of illegal robocalls will require multiple strategies. Strategies for:

- Authenticating the identity of legitimate callers and providing information to end users about legitimacy of callers.
- Providing information and tools to end users so that they can block the calls that they do not want to receive and allow the calls they do want to receive.
- Detecting illegal robocalling campaigns.
- Blocking illegal calls in the network before they are delivered to end users.
- Tracing back to the source of illegal robocalls so that action can be taken.

Carriers may make new investments in additional network capabilities, data analytics and additional staff to conduct traceback activities and to work with enforcement agencies. Companies may need to consider how to recover the costs and they have several options. See Attachment 1 for a description of the cost recovery mechanisms available to the industry.

Work Group	**Cost Impact Areas**
Authentication (WG1)	New network upgrades to sign and verify calls; upgrades to supporting operations support systems; certificate management.
Empowering Consumer Choice (WG2)	Feature development to pass information to end user devices; risk scoring to help customers make informed choices; call disposition options that reflect consumer's needs; feedback to solution providers.
Detection, Assessment, Traceback, and Mitigation (WG3)	Big data analytics and tools for identifying robocalls; scalable blocking capabilities; improved and accelerated robocall traceback; "do-not-originate" solution.

Attachment 1

Options to Support a Sustainable Long-Term Approach To Combatting Robocalls

A service provider's robocall mitigation costs will vary dependent on the technical architecture of a provider's network, the size of their network, the solutions they choose to employ, and the business relationships they have with their vendors and third party solution providers.

Some robocall mitigation solutions may only have a short life, and as the industry implements mitigation capabilities, robocallers will adapt and seek to work around solution as implemented and find new approaches. This "arms race" could continue until the cost of the workarounds become so high that the perpetrators move on to other opportunities.

Ideally, a strategy will not only cover the costs associated with the onetime costs and short term initiatives, but will have the flexibility to cover longer term initiatives and associated costs. A cost recovery strategy should also consider company specific costs as well as any costs associated with shared industry solutions or resources should they exist.

These strategies fall into three broad categories: 1. Congressional Appropriations, 2. Subscription Services, and 3. Surcharges/Fees Levied across the Customer Base

Congressional Appropriations

The Industry and the FCC could together ask Congress for appropriate funds to cover funding for an FCC managed "Do Not Originate" database.

Subscription Service

In this case, customers are given the option to subscribe to a basic service or a premium service. A basic service could include standard call blocking, call logging, and illegal call reporting features. A premium service could include optional robocall protection features such as a fraudulent call threat score and call treatment options.

Surcharges/Fees Levied Across the Customer Base

A small surcharge or fee could be applied to the customer's monthly bill for the entire customer base. Such a fee could be collected as a separate "Robocall Mitigation Fee" or could be added to existing fee categories, such as the "Cost Recovery Charge". Robocall mitigation benefits all users and this approach will allow the robocall mitigation costs to be spread over the largest base. This could be structured similar to the LNP recovery which allowed for the recovery of (1) shared industry costs, costs incurred by the industry as a whole; (2) carrier-specific costs directly related to robocall mitigation implementation. Shared industry cost would be costs incurred by the industry as a whole, such as those incurred to build, operate, and maintain the databases. Carrier specific costs would be costs carriers incur specifically in the provision of Robocall mitigation tools and processes. The carrier specific costs should be demonstrably incremental costs.

Attachment 2

Blocking Safe Harbor Statement

Question: When is it appropriate for a carrier to block a call that it has determined to be an unwanted or illegal call?[1]

Overview: Customers may not want to receive a significant number of calls - some are illegal but many are just unwanted. The FCC has made clear that carriers are authorized to block unwanted calls at the customer's request. In its September 30, 2016 Public Notice, the FCC stated "In the 2015 Omnibus TCPA Order, the Commission clarified that nothing in the Communications Act prohibits voice service providers from offering their customers such blocking tools when the customer requests it." However, in some scenarios the rules are not quite as clear and may require a clarification or declaratory ruling from the FCC.

"Blocking" in this context can take a variety of forms, including but not limited to responding to inbound requests with a variety of different SIP responses (including "486" busy responses) or playing an inbound tone or announcement in either a pre-answer or post-answer state.[2]

Requests from Consumers who do not want to receive unwanted calls

The only time a carrier should block an unwanted call is at the request of the end user customer who does not want to receive the call. The FCC has made clear that carriers are authorized to block unwanted calls at the customer's request. In its September 30, 2016 Public Notice, the FCC stated "In the 2015 Omnibus TCPA Order, the Commission clarified that nothing in the Communications Act prohibits voice service providers from offering their customers such blocking tools when the customer requests it." For example the end user consumer will be able to block based on call information as specified in the standardized framework for delivering information from the network to the device. For more information see the Empowering Consumer Choice section of the final Robocall Strike Force final report.

Authorization to block by the subscriber of a spoofed number

When a number is "spoofed" it shows the name and number of the subscriber on the recipient's caller ID in an attempt to appear like the call is coming from a trusted party. In many cases, the subscriber to whom the spoofed number is assigned uses the number for incoming calls only, such as a call center, government agency, or emergency alert center. IRS numbers are often targets of this type of spoofing because it has a great many numbers dedicated to receiving calls only. The FCC clarified in its September 30, 2016 Public Notice that carriers may block calls from these numbers at the customer request.

"We clarify here that voice service providers may block such calls when requested by the spoofed number's subscriber, e.g., a government agency such as the IRS. Such calls are presumptively

---

[1] An illegal robocall is one that violates the requirements of the Telephone Consumer Protection Act of 1991, 47 U.S.C section 227 and the related FCC regulations implementing the Act. 47 C.F.R 64.1200 *et seq.* and the Telemarketing Sales Rules 16 C.F.R. section 310. In addition, a robocall made for the purpose of defrauding a consumer is an illegal robocall under a variety of federal and state laws and regulations.

[2] Nothing in this document is intended to affect the rights to block traffic in conformance with the terms of commercial agreements.

spoofed and thus likely to violate the Commission's anti-spoofing rules. Moreover, the spoofed number's subscriber has a legitimate interest in stopping the spoofed calls – in light of the significant reputational damage and other harms they cause.

Further, consistent with the 2015 Omnibus TCPA Order, consumers can be presumptively deemed to have consented to the blocking of calls when the number's subscriber has requested it; we do not believe any reasonable consumer wishes to receive calls that display a spoofed Caller ID and have no purpose other than to annoy or defraud. We base our conclusion on evidence that consumers' top complaint with the Commission is unwanted robocalls and the well-known use of trusted numbers to lure consumers into fraud schemes."

In addition, a carrier should be permitted to block calls that spoof unassigned numbers, if it has confirmed with the carrier that owns that number that it is not assigned to any end user.

Calls that have been identified as illegal robocalls

Blocking calls in this situation is less clear. While the FCC clarified in its September 30, 2016 Public Notice that service providers can block calls displaying a spoofed number when requested by the spoofed number's subscriber, the commission also should clarify that service providers may also block calls that have been determined to be illegal robocalls. Similar to the calls addressed in the Public Notice, it follows that consumers can be presumptively deemed to have consented to the blocking of calls when the call has been identified as illegal.

The industry effort to identify and trace the robocalling campaigns is showing progress and efforts are being stepped up. And, while work is being done to shorten the time between identification and stopping the campaign, millions of these illegal calls can get through to consumers before an enforcement agency can issue a cease and desist. So, the FCC should clarify that blocking presumptively illegal calls is one of the tools carriers are permitted to use to provide consumers additional relief. When a service provider blocks calls it should take reasonable steps to confirm, to the extent possible, that the calls are illegal. Examples of reasonable efforts include but are not limited to, soliciting and reviewing information from other carriers, performing historical and real-time call analytics, making test calls, contacting the subscriber of the spoofed number, inspecting the media for a call (audio play back of the Real Time Protocol stream to understand the context of the call), and checking customer complaint sites. Additionally, there should be a safe harbor for entities who act in good faith by following the identification and verification process if they inadvertently block a legitimate call. Finally, 47 C. F. R. section 64.2105 should be amended to state that calls blocked to protect consumers from receiving illegal robocalls will not be considered when evaluating the long distance call completion rates.

Note: This guidance is based on regulations and processes that are in place as of October 7, 2016 and may need industry review and revision in the future.

Attachment 3

FCC Clarification on Sharing Information

Background and Issue Statement: Various members of the Strike Force report that when conducting traceback investigations in the past, they frequently encounter upstream carriers that decline to provide information about the source of suspicious traffic that they have sent to downstream carriers. These upstream carriers often assert that providing the requested information would violate privacy principles, such as the CPNI provisions of 47 U.S.C. Section 222, or that it would violate the confidentiality provisions in their contracts with their customers.

Proposed Guidance:

The FCC should clarify that:

i. There is no legal barrier to performing traceback investigations;
ii. Industry is encouraged to participate in good faith traceback investigations, consistent with industry best practices.

The FCC should declare that it is sound public policy to:

i. Include in service provider agreements terms that: require compliance with the federal Telephone Consumer Protection Act (TCPA); and authorize either service provider to such an agreement to disclose to a third party provider or industry group performing a traceback of Suspicious Traffic using industry best practices the identity of any upstream provider sending Suspicious Traffic, and other pertinent information to determine what action to take regarding this traffic.

Specifically, the FCC should address the following questions:

Question No. 1: Does anything in Section 222, or anywhere else in the Act or the FCC's rules, prevent carriers from sharing information with one another about their source of Suspicious Traffic[3] with other carriers who are investigating the traffic?

Proposed Recommended FCC Clarification: No. To the extent the source is a customer (whether wholesale or retail), information relevant to resolving or mitigating suspicious traffic originated or passed on, can be shared under Section 222 because subpart (d)(2) of that statute permits sharing CPNI in order to "protect the rights of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." Further, disclosing this information in the context of investigating suspicious traffic does not violate the Section 222(b) prohibition on disclosing "carrier proprietary" information.

---

[3] "Suspicious Traffic" has been defined by carriers to mean: "[V]oice calls or telecommunication sessions that transit one or more carrier networks and that are deemed suspicious due to evidence that they may be associated with abusive, unlawful, or fraudulent activity. That evidence can include credible documented customer complaints associated with the traffic, substantiated reports about the content of the calls, or technical characteristics (including but not limited to lack of header information, volumetric anomalies, or Calling or Called party modification) that providers have identified as associated with fraudulent, abusive, or unlawful traffic. Carriers should work collaboratively to further develop this definition on an as-needed basis."

Question No. 2: Should providers be able to raise contractual provisions prohibiting the disclosure of confidential information in contracts or agreements governing exchange of traffic as barriers to providing information to third parties investigating?

Proposed Recommended FCC Declaration: The FCC should find that, as a matter of sound public policy, contractual provisions that restrict a provider's ability to cooperate with a third-party provider or industry group's traceback process are not in the public interest.

In determining what constitutes "industry best practices" with respect to (i) when tracebacks are appropriately initiated (including triggering criteria) and (ii) responding promptly to traceback requests, the Commission encourages carriers to rely on the practices followed by members of industry trade associations or other groups dedicated to robocall mitigation.

Attachment 4

Robocall Definition

Assignment: Describe/define the robocalls to which mitigation techniques will apply.

Issue Statement: The Strike Force's technical working groups (Nos. 2 and 3) have requested guidance on what types of calls should be subject to the mitigation measures they are developing. Working Group No. 2 is exploring ways to better empower consumers to control what calls ring on their devices. Working Group 3 is exploring network-based solutions, including better traceback techniques to identify the sources of suspicious robocalls and possible solutions where network providers would not accept certain traffic onto their networks.

Background on Lawful versus Unlawful Calls: Distinguishing between lawful and unlawful calls requires legal analysis that cannot be done real-time, and in some cases is unclear *post facto*. The Telephone Consumer Protection Act prohibits many calls that have prerecorded messages or are initiated with autodialers or the functional equivalent but it also authorizes such calls in many contexts. The legality of a call depends on the nature of the called party (wireless customers have greater protections than wireline customers), the nature of the calling party (e.g., Congress has authorized political robocalls to wireline customers), and whether the purpose of the call falls into an established exemption (e.g., the FCC has exempted certain calls from financial institutes and healthcare providers). Those complexities and exemptions, combined with the fact that *any* robocall is lawful if the called party has previously expressly consented to receive it, mean it is not possible to apply technical criteria to determine whether or not a robocall is lawful.

Proposed Guidance: What constitutes a call potentially subject to mitigation depends on the context of the mitigation measure. While not exhaustive, below are three mitigation contexts which require separate guidance as to what calls should be targeted.

A. Consumer-Directed Blocking/Filtering Tools.

A consumer is permitted to block or filter any type of call, regardless of whether it is lawful or unlawful, either by directly identifying the calling parties from whom he does not want to receive calls or by opting into a tool that will block or filter certain types of calls on his behalf. The FCC has confirmed that there is no obstacle to offering customers tools to block or filter unwanted calls as long as they choose such tools through an informed opt-in process.[4] The FCC also strongly encourages voice providers and independent blocking services to avoid blocking calls from public safety agencies.[5]

Here is a proposed definition of the traffic subject to consumer-directed blocking or filtering tools:

Unwanted Traffic. Any calls that individual consumers decide (either by directly identifying the calls or by opting into a particular blocking or filtering tool) that they do not want completing onto devices they own or by the nature of the device (such as carrier provided mail) be considered a terminating end user destination.. This category of traffic may vary for different consumers or different tools and each consumer may have different preferences.

[4] *See* Declaratory Ruling and Order, CG Docket No. 02-278 (June 18, 2015), ¶¶ 154-63.

[5] *Id.*, ¶ 157.

B. Traceback.

Tracebacks should be conducted where (i) the traffic under investigation meets criteria established by Group 3 to ensure that traceback resources are focused on traffic affecting substantial numbers of consumers, and (ii) the initiator of the traceback has a *bona fide* basis to suspect the traffic is unlawful. This guidance addresses only the criteria that should be present to establish a presumption of unlawfulness under (ii) above sufficient to trigger a traceback investigation. Separately, Group 3 may develop criteria for what mass calling events should be targeted in order to maximize the effectiveness of traceback resources. An open issue for discussion and research is what traceback participants should do once they isolate the source of the traffic.[6]

There are two types of criteria that support initiating traceback investigations:

1. Substance of Calls Provides a Basis to Suspect Fraudulent or Abusive Intent or a TCPA Violation. A traceback is appropriate where the initiating party has a *bona fide* basis to suspect that traffic affecting its network or its customers is associated with attempted fraud, is abusive (e.g., is associated with a denial of service attack), or includes calls that are violations of the TCPA. These criteria can be based on a variety of sources, including but not limited to customer complaints received directly by voice providers, customer complaints made to the FTC or FCC, reports about unwanted calls made to Internet sites, or direct experience that a voice provider has with the call (such where an employee has received the call and reports on its substance.).

2. Presence of Technical Criteria Known to Be Associated with Unlawful Traffic. Another basis for initiating a traceback investigation is where the traffic at issue has technical characteristics that are reasonably known to be associated with unlawful traffic. Those criteria may include, but are not limited to, lack or modified signaling and/or header information, volumetric anomalies, or certain Calling or Called party modifications. For example, calling parties who are spoofing unassigned telephone numbers may be deemed sufficiently suspicious to support initiating of a traceback investigation. These criteria should be updated as learning develops and should only be shared with other carriers or entities actively involved in traceback functions; given that illegal robocallers are likely to find ways to defeat the trigger if they know what it is.

Based on those criteria, here is a proposed definition of what "Suspicious Traffic" should be subjected to traceback investigations:

Suspicious Traffic. Suspicious Traffic means voice calls or telecommunication sessions that transit one or more carrier networks and that is deemed suspicious due to evidence that it may be associated with abusive, unlawful, or fraudulent activity. That evidence can take a variety of forms, including complaints associated with the traffic, reports about the content of the calls, or technical characteristics (including but not limited to lack of header information, volumetric anomalies, or Calling or Called party modification) that traceback participants have identified as associated with fraudulent, abusive, or unlawful traffic. Carriers should work collaboratively to further develop this definition on an as-needed basis.

[6] To the extent the originator of suspicious traffic justifies it as compliant with the TCPA and other applicable laws, there is obviously no basis to stop such traffic. A separate question beyond the scope of this submission is what procedures should be in place to determine when it may be appropriate to block suspicious traffic if its source has been isolated and the source fails to justify it.

C. Potential Network-Based Blocking.

Group 3 is also exploring potential mitigation techniques where network providers may decline to accept certain traffic on their networks, such as traffic identified under a "Do Not Originate" framework as spoofing unassigned numbers or numbers assigned to legitimate callers. This type of mitigation is distinct from the consumer-directed blocking/filtering tools discussed in Section A above because it would prevent the mitigated calls from reaching all called parties, regardless of whether they have opted in to being protected from such traffic. Guidance on when such mitigation techniques should be employed will depend on the details of mitigation techniques reviewed by Group 3.