Best Practices for Terminating Voice Service Providers using Caller ID Authentication Information

NANC Call Authentication Trust Anchor Working Group

Table of Contents

Best Practices for Terminating Voice Service Providers using Caller ID Authentication Information

1. Introduction

Fighting illegal robocalls is a top consumer protection priority for the Federal Communications Commission (FCC), and call authentication is an important part of solving this critical challenge. With the passage of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act, Congress expressed its support for a robust call authentication system.[1]

The FCC's Wireline Competition Bureau has called upon the North American Numbering Council's (NANC) Call Authentication Trust Anchor (CATA) Working Group (WG), to develop a set of best practices relating to how terminating voice service providers can best protect their subscribers using caller ID authentication information. Specifically, they directed the NANC to address the following:

1. Identify and explain how STIR/SHAKEN caller ID authentication information is being or has been used by voice service providers and others to combat illegal robocalls.
2. Recommend a set of best practices for terminating voice service providers to reference regarding both the use of STIR/SHAKEN caller ID authentication information to protect subscribers and protecting subscribers who fall outside of the STIR/SHAKEN framework; including but not limited to the following:
    - Means by which terminating voice service providers can use the STIR/SHAKEN caller ID authentication information included in calls they receive to best protect their subscribers, including elaborating on how that information can improve call analytics and blocking strategies.
    - Techniques that do not rely on STIR/SHAKEN caller ID authentication information that terminating voice service providers could employ to protect consumers.
    - Whether, and if so, how, STIR/SHAKEN caller ID authentication information—including but not necessarily limited to verification results—should be shared with call recipients.
        - If STIR/SHAKEN caller ID authentication information should be shared with call recipients, recommend whether this practice should be standardized.

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

2. Report

The STIR/SHAKEN framework with caller ID authentication provides the long-term means to protect subscribers by identifying parties responsible for generating illegal robocalls. However, many Voice Service Providers (VSPs) are still implementing the STIR/SHAKEN framework. Terminating service providers, when implementing the framework, should integrate STIR/SHAKEN with additional measures such as call analytics and blocking solutions. Terminating VSPs that leverage multiple techniques to detect and stop illegal robocalls are better positioned to protect their subscribers and improve their current call experience.

In addition to the best practices presented in this document, terminating VSPs should be aware of previously published best practices: *Best Practices for the Implementation of Call Authentication Frameworks* and *Deployment of STIR/SHAKEN by Small Voice Service Providers*. Terminating VSPs may experience that originating VSPs have not effectively implemented all best practices and should monitor for illegal robocalls.

This section provides background information that supports the best practices for a comprehensive approach to detect and act upon illegal robocalls delineated in Section 3. Section 2.1 focuses on STIR/SHAKEN and how authenticated caller ID information can be leveraged to combat illegal robocalls. Section 2.2 presents other ancillary STIR/SHAKEN specifications that need to be considered by a terminating VSP. Section 2.3 describes a comprehensive list of additional techniques that can be used with, or without, a STIR/SHAKEN implementation to combat illegal robocalls.

2.1. STIR/SHAKEN Caller ID Authentication Information for combatting illegal robocalls

STIR/SHAKEN at its core is a technology and protocol that combines two fundamental processes. First, the authorization of an entity in the use of a telephone number and second, the authentication and verification that proves the entity that initiated a call is the authorized entity. In both the standards surrounding STIR/SHAKEN and previous CATA Working Group reports, processes and policies have been discussed that tie into those fundamental authorization and authentication techniques. These adapt the traditional flows and business models that have developed in the telephone eco-system and integrate a layer of trust in the telephone identity that can be securely and confidently determined at the point of verification.

As the telephone eco-system has evolved its capabilities from simple point-to-point telephone calls to highly sophisticated telephony applications, the security of the telephone identity has not evolved with those capabilities. Persistent unwanted robocalls, sometimes malicious, have eroded trust in the public telephone network. Illegally falsifying the originating telephone number or caller identity exacerbates the problem. It is often a necessary means to achieve a desired application without the need to use a traditional telephone device to place a call; however, policies associated with authorization and authentication security were not prioritized as these capabilities were developed. STIR/SHAKEN caller ID authentication is an important tool for restoring that missing security and trust in the network because it can be used to verify a caller’s right to use the originating telephone number.

Customer vetting also should be part of any robocall mitigation program and should precede establishment of new service by a VSP. The TN Validation process is a separate best practice as outlined in *Best Practices for the Implementation of Call Authentication Frameworks* by this Working Group.

The efficacy of STIR/SHAKEN is currently constrained by non-ubiquitous implementation. As noted by the *TNS 2021 1H Robocall Investigation Report*[2], tier-1 Service Providers have deployed the call authentication framework with more than 50% of the total calls in June 2021 signed and validated, up from 35% at the beginning of the year. While the eco-system is still on the uphill climb to achieve the "critical mass" of signed and fully attested calls to achieve "trust" in the network, the Working Group believes that ongoing efforts to bring all participants (particularly U.S, and NANP participants) under the umbrella of the deployment of STIR/SHAKEN, makes this goal achievable. There are two general categories of techniques to focus upon, those that use STIR/SHAKEN signing more generally, and those that depend upon the more ubiquitous implementation of STIR/SHAKEN.

2.1.1. Use of STIR/SHAKEN signatures

Currently, there are techniques that can utilize each signature independently. At the point of verification, if the digital signature is correct and the attestation level is "A", one of the primary means to help the consumer is to display that information to them as the call is received. SHAKEN provides information that can be used to notify an end user that the calling number was correct, and that the call was authenticated. Call analytics engines use recent information about the calling telephone number such as caller registration information, calling patterns (e.g., a high percentage of short duration calls), and customer complaints to help determine the intent of the call.

Usually call authentication information is displayed to the end user with a check mark (by sending "verstat=TN-Validation-Passed" to the consumer's handset, an enterprise's PBX, etc.) or a "[V]" (by modifying the caller display name) when the call receives full attestation. If supported by the end user equipment, the terminating service provider may send the SIP Identity headers to the end user. There is more variation in display or treatment when communicating information about the intent of the caller. Depending upon the call analytics engine, a call likely to be fraudulent or unwanted may be blocked, sent to voicemail, or labeled to indicate spam, fraud, or scam. Some call analytics engines also provide other labels such as "telemarketer".

The certificate used to sign a SHAKEN PASSporT contains a Service Provider Code (SPC). The SPC, as registered with the Secure Telephone Identity (STI) Policy Administrator, uniquely identifies the service provider that created the PASSporT which could provide useful information for ascertaining the bad actors in the call path.

[2] https://tnsi.com/tns-robocall-report-americans-deluged-with-80-billion-unwanted-calls-over-past-year-but-they-arent-coming-from-tier-1-carriers/

2.1.2. Use of STIR/SHAKEN signatures with more ubiquitous deployment

The eco-system will eventually reach a “critical mass” where there is broad deployment of: STIR/SHAKEN; Vetting and TN Validation procedures; and policies and techniques to provide “A” attestation levels for indirect (often referred to as enterprise) call scenarios. Whether as a user feature or a broader policy, the ability to filter calls that do not have “A” attestation can become a tool for providing more robust subscriber-protection capabilities. The ability to utilize STIR/SHAKEN parameters from VSPs that utilize best practices of customer vetting can help put “trust” in the telephone number. STIR/SHAKEN will allow for more robust abilities to either trust the caller or perform traceback because an illegal caller can be more easily identified.

It can be assumed, however, that illegal robocalls will persist after STIR/SHAKEN call authentication technology is more broadly deployed. Illegal robocallers may adapt their calling patterns to avoid call labeling and blocking and evade prosecution. In fact, call analytics providers are already experiencing VSPs that do not have robust customer vetting processes and are allowing upstream VoIP service providers to use legitimate telephone numbers to perpetuate illegal robocalling campaigns by spreading calls over thousands of telephone numbers to avoid detection. It also remains to be seen how call analytics providers and VSPs will adapt their practices to incorporate new information made available by STIR/SHAKEN call authentication.

There is not necessarily tightly integrated call analytics and authentication designs yet in all service provider networks. Some service providers may have deployed STIR/SHAKEN call authentication and verification functions separately from call analytics functions and from different vendors. There may not be much or any integration of the results of a SHAKEN call verification with the results of anti-robocalling analysis in provider networks using disparate vendors for authentication and analytics functions. In environments where both call authentication and analytics functions are provided by a single vendor, there may be tighter integration of SHAKEN verification information with analytics algorithms. The same effect can be achieved with independent call authentication and call analytics vendors when there is significant coordination.

SHAKEN verification can provide a rich set of inputs for anti-robocalling analytics. Absence or presence of a SHAKEN call signature can be useful input. Successful or failed verifications can also provide useful input. Beyond success or failure, the information elements of the call signature can provide additional useful inputs to anti-robocalling analytics.

The attestation indicator “attest” in the payload of a SHAKEN PASSporT can have a value of “A” (full), “B” (partial), or “C” (gateway). The value of the attestation is a key indicator of what the call signer intends for the call verifier to know about the call signer’s relationship to the caller and their telephone number.[3] However, call analytics providers have seen use of “A” level attestation on telephone numbers that should not have such attestation (e.g., invalid telephone numbers). Voice service providers should follow the best practices identified in section 3.1 below.

[3] See ATIS-1000074 “Signature-based Handling of Asserted information using toKENs (SHAKEN)”

Early reports published by TransNexus, since the June 30, 2021, deadline to deploy STIR/SHAKEN, indicate robocalls signed using SHAKEN call authentication have been predominantly signed using a “B” (partial) or “C” (gateway) attestation.[4]

The “origid” field of a SHAKEN PASSporT is an opaque origination identifier with context local to the call signer (i.e., only the call signer knows what the “origid” is supposed to represent). By standard, “origid” should be a Universally Unique Identifier (UUID) but can be and sometimes is other values. Regardless of being a UUID or not, the value can help facilitate traceback and potentially provide additional information as input to analytics algorithms (e.g., a reputation score associated with an “origid” value).

Analytics providers can use the results of conventional analytics processing to learn whether patterns of SHAKEN attestation and origination identifier assignment are consistent with calls that result in lower or higher reputational scores.

In addition to the success or failure of verifications and the values of fields in the SHAKEN payload, there is additional information in the STI certificates used for verifying SHAKEN call signatures. The “Subject” of the certificate identifies the call signer. The “Issuer” of the certificate identifies the authority which signed the certificate issued to the ”Subject.” As with attestation and origination identifier, conventional analytics can be applied to information found in STI certificates including SHAKEN STI certificate extensions.

Typical anti-robocalling analytics products can provide call labeling, support blocking, and generate reports. It is not difficult to imagine that call analytics integrated with input from SHAKEN informational elements could identify the Subject and the Issuer of certificates associated with illegal robocall campaigns and automatically notify authorities such as state attorneys’ general and the FCC-sanctioned consortium responsible for traceback (currently the US Telecom Association’s Industry Traceback Group).

2.2. Ancillary technologies/techniques using STIR/SHAKEN

Several ancillary extensions have been added to the STIR/SHAKEN framework and base standards that cover calling use cases not explicitly covered by the initial standards. The following sections will briefly discuss the ancillary extensions and their planned usage. It is important that terminating VSPs consider supporting these ancillary extensions when implementing the STIR/SHAKEN framework to protect their subscribers from illegal robocalls.

2.2.1. Call Diversion

Call diversion is a complex topic with many variations but is an important subset of existing call features and applications that are widely used today. With respect to the discussion in this report, ensuring the accuracy of PASSporTs associated with forwarded calls is particularly important. Many traditional and advanced telephone services provide the ability to redirect a call from the called number to another destination based upon either the called party preference or an advanced application. For example, call forwarding is a basic call feature that allows users to

[4] https://transnexus.com/blog/2021/robocall-trends-july/

retarget a call from one telephone line to another. More complex scenarios such as a call center, may have sophisticated logic for redirecting a call many times in a session depending upon whom the caller may want to reach. The STIR/SHAKEN standards [ATIS-1000085] have defined the use of a “div” PASSporT which allows the additional call destinations to have a signed identity header containing the details of each diversion or redirection in the call path to keep the changing destination calling identity cryptographically secure.

2.2.2. 911 support

The STIR/SHAKEN framework standards for the signing of 911 calls was recently completed. These standards use the “rph” PASSporT for both 911 calls and 911 callbacks (e.g., calls from PSAPs to 911 callers in the case of a dropped call) to support both priority delivery of the calls and to help identify the caller properly for VSPs attacks and other uses for trusted identity in 911 cases. 911 systems are evolving from circuit switched to VoIP/SIP (IMSESINET/i3). Signing of the “rph” PASSporT for both 911 calls and 911 callbacks can only occur with IP end to end.

2.2.3. ETS support

Emergency Telecommunication Service (ETS) using public telecommunications networks is offered by government to authorized users for National Security/Emergency Preparedness (NS/EP) purposes, in support of the Government Emergency Telecommunications Service (GETS) and Wireless Priority Services (WPS).

GETS is one facet of ETS. GETS is a circuit-switched form of ETS for voice (and voiceband data) using PIN authorization, in which a user can invoke the service by dialing a GETS Access Number (GETS-AN) or GETS Number Translation (GETS-NT) from most phones connected to the Public Switched Telephone Network (PSTN). GETS provides priority treatment across originating, transit and terminating networks as described in [ATIS-1000057], Service Requirements for Emergency Telecommunications Service (ETS) in Next Generation Networks.

Wireless Priority Service (WPS) is a wireless form of ETS for voice (and voiceband data) using subscription-based authentication, in which a user can invoke the service by dialing a feature code from a WPS-subscribed mobile phone served by a public wireless network. WPS provides priority treatment across originating and terminating public wireless networks, including priority radio resource assignment upon call origination and termination.

2.2.3.1. Interaction with ETS

Per ATIS-1000074.v002, Signature-based handling of Asserted information using toKENs (SHAKEN), clause 5.3.4: Handling of Calls with Signed SIP Resource Priority Header Field, “For calls that contain a SIP Resource Priority Header (RPH) field, post STI-VS information may be passed for Call Validation Treatment (CVT) depending upon the value of the namespace parameter in the RPH field and in accordance with local policy and/or policy of the authority responsible for the specific service”.

Emergency Calls with a SIP RPH value in the “esnet” namespace may be passed for CVT depending upon local policy. National Security / Emergency Preparedness Priority Service

(NS/EP PS) calls with SIP RPH values in the “ets” and/or “wps” namespaces may also be passed for CVT depending upon local policy.

For operational considerations, see *ATIS-0300116, Interoperability Standards between Next Generation Networks (NGN) for Signature-Based Handling of Asserted Information Using Tokens (SHAKEN)*. An NS/EP call with an “rph” PASSporT that is successfully verified is treated as if it has a verified “shaken” PASSporT with an attestation level of “A”.

2.2.4. RespOrg and Toll-Free support

The STIR/SHAKEN framework [ATIS-1000093] standard supports the ability for RespOrgs to use “shaken” PASSporTs or provide delegate certificates to their customers for the purpose of fully attesting and signing toll-free calls.

2.2.5. Delegate Certificates

The STIR/SHAKEN framework [ATIS-1000092] supports the ability to provide and sign calls with delegate certificates for the purposes of providing proof of the right to use telephone numbers or for supporting Rich Call Data (RCD) associated with a telephone number. Delegate Certificates depend upon Vetting and TN Validation techniques discussed in the second CATA Working Group report related to enterprise techniques discussed in [ATIS-1000089].

2.2.6. Non-IP Call Authentication

The STIR/SHAKEN framework supports two mechanisms of transmitting call authentication information for non-IP calls [ATIS-1000095] and [ATIS-1000096].

2.2.7. Cross-Border SHAKEN

The STIR/SHAKEN framework [ATIS-1000091] presents a framework for supporting both international (+1 country code), as well as other international country codes or regulatory domains. There is still more work to do in this space including agreement on cross-border policies for accessing approved CA Root certificate lists and Certificate Revocation Lists (CRLs).

2.3. Non-STIR/SHAKEN Techniques for combatting illegal robocalls

As previously mentioned, STIR/SHAKEN deployment is one important technique for terminating VSPs to help identify the source of illegal robocalls. However, terminating VSPs should leverage additional techniques to protect their subscribers from illegal robocalls. Many of these additional techniques can be initially deployed independently of STIR/SHAKEN and then enhanced to leverage authenticated caller ID information when available.

2.3.1. Do Not Originate, Unassigned, Unallocated, Illegitimate Number Call Blocking

An obvious and straight-forward technique for fighting illegal robocalls is to avoid terminating calls that show numbers in the caller IDs that should not be originating phone calls. There are specific criteria for why a number could be legitimately blocked from being terminated.

These include numbers that are:

- On an industry Do Not Originate (DNO) list[5]
- Unallocated (by the numbering plan administrator)
- Disconnected
- Unassigned
- Invalid

2.3.2. Vetting and TN Validation

Vetting and TN Validation are two tools that are part of a general framework for the best practices of association of assigned numbers to legitimate subscriber(s) or customer(s). Many details of this are set forth in the CATA Working Group report *Best Practices for the Implementation of Call Authentication Frameworks*.[6] Vetting efforts involve verifying the identity of voice customers at the time a business relationship is established (i.e., before customers begin sending traffic onto a network). Vetting the identity of retail customers is advisable, particularly enterprise or other business customers, but vetting is particularly important in wholesale relationships. The latter includes scenarios where a VSP supports a Value-Added Service Provider (e.g., cloud telephone application provider) with right-to-use telephone numbers. Vetting customers may include collecting the addresses of physical locations, trade names, contact persons, contact telephone numbers, and contact email addresses. If the customer is a VSP, their status as a Form 499 filer might be ascertained. TN Validation is the process of making sure the subscriber or customer has the right-to-use of the telephone number, including for legitimate spoofing purposes, and therefore can use it to originate a call with that calling identity, whether as part of a retail line of service or as part of an application, CPaaS or PBX type of service.

2.3.3. Call Analytics Engines

The goal of call analytics engines is to provide a service to customers and subscribers that can help mitigate illegal and fraudulent calls and to provide timely, relevant, and accurate information to the user so they can make a real-time decision whether to answer a call. This

[5] DNO lists contain telephone numbers that the authorized user does not use for originating calls. There are several industry DNO lists, including the ones managed by the Industry Traceback Group (ITG) and Somos.

[6] *Best Practice for the Implementation of Call Authentication Frameworks*, NANC Call Authentication Trust Anchor Working Group, Sections 3.13 and 3.14.

approach helps to protect consumers and to empower them with control over the calls they receive.

Call analytics engines function like a trusted credit reporting service continuously collecting data from multiple sources. They analyze calling numbers that have been internally or externally vetted and have been TN-validated as described in Section 2.3.2, use sources of information regarding DNO or legitimate numbers as described in Section 2.3.1, or use various real-time call analytics information such as:

- Calls of short duration but in high volumes;
- Calls that fail to pass voice CAPTCHAs;[7]
- Calls to honeypots;[8]
- Calls that were reported as unwanted by subscribers to call analytics engines; or
- Calls that were reported as unwanted by subscribers to the FCC or FTC.

These call analytics techniques rely upon a mix of recent historical data and real-time intelligence – making use of known legitimate and malicious behavior to project reputations on virtually any telephone number.

Service Providers and subscribers can leverage a call analytics engine to track and score each incoming telephone number with a reputation, and then allow their call processing applications to apply the appropriate call treatment based upon the analytics response. There are multiple options that may be available for call treatment, for example:

- Calls can proceed with no treatment for positive reputation;
- Calls can be blocked in the network (calls that are highly likely to be illegal such as invalid/malformed TNs, DNO, not allocated, etc.);
- Calls can be sent to voicemail (medium risk calls); or
- Calls can be labeled with a Spam/Scam indicator (warn the subscriber of potential nuisance calls).

Call treatment requires a balancing of considerations to avoid undermining the effectiveness of call analytics engines in mitigating harmful and fraudulent calls for the sake of additional transparency for consumers or call originators. Effective redress options exist today, and all parties are working to improve their efficiency (i.e., minimize false positive/false negative rates).

Call analytics engines need to evolve in response to emerging bad actor trends, such as neighbor spoofing, which uses number randomization techniques that are hard for statistical analytics to detect. For example, neighbor spoofing and variations of neighbor spoofing, such as snowshoe spamming, occur when the calling party identity received is randomized but uses the NPA-NXX that matches or closely matches the area code and exchange of one's own phone number.

[7] Voice CAPTCHAs typically require the calling party to enter a digit or series of digits to test whether the calling party is a human or auto dialer.

[8] Honeypots are destinations that should not receive calls. A call placed to a honeypot may indicate that the calling party is placing calls to randomly or sequentially selected destination numbers.

2.3.3.1. Service Provider Network Call Analytics Engines

Some service providers use call analytics engines in their network. In that scenario, where the subscriber may have little control over the call treatment behavior, care must be taken by the service provider to minimize the likelihood of call treatment being applied to wanted calls, especially emergency calls. This type of analytics most often results in blocking rather than labeling.

While a robust call analytics engine coupled with STIR/SHAKEN authenticated caller ID information is recommended, terminating VSPs can deploy some simpler techniques independently. For example, some calling number types listed in the previous section like DNO or invalid/unallocated telephone numbers are relatively easy to identify and relatively static, potentially requiring only monthly routing updates coupled with a calling telephone number screening and/or blocking solution.

2.3.3.2. Subscriber Call Analytics Engines

Some subscribers can set up call analytics engines for their phone line. These call analytics engines may be offered by their service provider or a third party. For mobile subscribers, call analytics engines are sometimes set up by installing an application on their mobile device. For non-mobile subscribers, call analytics engine setups vary widely.

Call treatment behavior is sometimes configurable by the subscriber. For example, the subscriber is sometimes able to override the call treatment behavior for a specific calling number when a call is inaccurately classified as unwanted.

2.3.4. Subscriber Device Features

Some devices allow subscribers to block calls on the device itself. Wanted, legal unwanted, or illegal unwanted calls may be intentionally or unintentionally (i.e., by default) blocked or routed to voicemail.

2.3.4.1. Calling Numbers Block Lists

Some devices can block calls from specific calling numbers. The subscriber manages the list of blocked calling numbers on the device or through an online portal in the case of fixed (landline) services.

2.3.4.2. Anonymous Call Rejection

Some mobile devices and some fixed services have an Anonymous Call Rejection mode/feature which can be enabled/disabled by the subscriber. When enabled, the mode/feature typically blocks calls where the calling party has blocked display of the calling number. Some services allow the subscriber to choose whether the call is blocked or routed to voicemail.

2.3.4.3. Do Not Disturb

Some devices have a Do Not Disturb mode which can be enabled/disabled by the subscriber. When enabled, the device typically blocks calls from calling numbers not present on a subscriber defined allow list. The allow list is often the subscribers contact list or a subset of the contact list. Some devices allow the subscriber to choose whether the call is blocked or routed to voicemail. Some devices can be configured to allow calls from calling numbers not present on the subscribers allow list when Do Not Disturb mode is enabled if multiple calls are received from the same calling number in a short period of time.

2.3.5. Traceback

Participation in and cooperation with the Industry Traceback Group (ITG) is important to bring accountability to the service provider ecosystem in the U.S. The Industry Traceback Group, currently led by USTelecom, conducts tracebacks on behalf of the industry through a Secure Traceback Portal. The ITG traceback process automatically generates and sends email notifications to upstream providers that fall within the call path of a suspected illegal robocall that is being traced back. When the ITG process identifies the originator of suspicious robocalls, or a point of entry routinely responsible for bringing illegal traffic into the U.S., the ITG asks the relevant provider the steps it is taking to mitigate the illegal traffic. Mitigation typically includes terminating the customer; it also can involve enhancing Know Your Customer measures going forward. The ITG also works closely with federal and state law enforcement and other stakeholders, providing information regarding the domestic and international providers identified most often in tracebacks.

3. Best Practices

The best practices recommended in this report for terminating VSPs were developed based upon industry expertise and experience, to assist in the overall objective of mitigating robocalling when implementing call authentication frameworks. These best practices:

1. Are considered voluntary and do not imply mandatory implementation, nor should they be mandated, to ensure Service Providers have the flexibility and speed to respond to evolving issues.
2. Were developed through rigorous deliberation and industry consensus by a broad set of stakeholders.
3. Have been proven through actual implementation and are more than just “good ideas”.
4. Address classes of problems, rather than one-time issues.
5. Do not endorse specific commercial products or services.
6. Should not be assumed to apply in all situations or to all industry types.

Terminating service providers should evaluate and implement the best practices they deem appropriate. The recommendations in this report can help inform a specific organization’s best practices. Additionally, organizations should institutionalize the review of these best practices as part of their operational processes and assess, on a periodic basis, how implementing selected best practices might assist in the overall mitigation of robocalls.

3.1. Best Practices for Terminating Service Providers to Protect Subscribers

The following best practices are listed in two categories. Near-term best practices are those that can be implemented at present. Longer-term best practices are those where standards work is still in development or where the absence of ubiquitous deployment of SIP networks negatively impacts the efficacy of the best practice.

Near-Term Best Practices

1. Display to the subscriber a STIR/SHAKEN verification indicator for calls with an attestation level of "A."[9]
2. Employ or make available to the subscriber, complementary analytics to identify calls that are highly likely to be illegal or unwanted.
3. Display call labels to subscribers and/or employ diversion techniques that enable redirection of calls to alternate destinations such as voice mail.
4. Offer to subscribers call treatment options such as block lists, anonymous call rejection, or do not disturb.[10]
5. Block calls that are highly likely to be illegal before they reach subscriber premises equipment (e.g., calls from invalid codes, calls from unallocated or unassigned numbers, and calls on a do-not-originate list).

Longer-Term Potential Best Practices

1. Use analytics algorithms to identify patterns of information found in SHAKEN PASSporTs (e.g., attestation and origination identifier assignments) that may provide better accuracy for reputational scores. Note that "reputation scores" can apply at the individual user level (i.e., as determined by the calling party number and origination identifier), as well as at the service provider level (i.e., associated with all calls from a service provider using a given STI certificate).
2. For calls with a signed Resource Priority Header (RPH) PASSporT, use the RPH field for Call Validation Treatment when terminating calls to a PSAP, or terminating callbacks from PSAPs.

Because not all illegal calls are spoofed, SHAKEN information should be communicated with analytics or provided pursuant with information to educate customers on the meaning and any limitations of the verification display. Information provided to end users need not be

[9] Service providers should have flexibility to potentially display an indication of "A" attestation in a manner compatible with their technology and the devices typically used by end users of their services. For example, verification display on a smart phone may differ from display on caller ID devices used with fixed line services or caller ID to the TV. Irrespective of the verification symbol used, end users should be informed about any verification display associated with their service, including meaning the display conveys and what it does not convey (i.e., the intent of a caller). End users should also be informed that an "A" attestation applies to the calling telephone number and not necessarily to the name of the caller.

[10] Call treatment options may differ between wireline and wireless networks and from provider to provider. Differences may be based on technology capabilities or product decisions. For example, some wireless services have the capability to access address books to determine whether the caller is included in the called party's address book.

standardized. Display options have evolved and will continue to change based upon new options and customer demand. As a result, standardization should not be required because it would likely stifle future innovation.

3.2. Issue for Further Study

There is recognition that enterprise customers may benefit from more information than a simple SHAKEN verification result (e.g., “verstat=TN-Validation-Passed”, “verstat=TN-Validation-Failed”, or “verstat=No-TN-Validation”) parameter. Enterprises may want to perform their own analytics to verify the identity of the calling party and more directly combat fraud and abuse. However, the universe of enterprises and their technical capabilities is quite diverse and complex, thus complicating recommendations that go beyond currently sharing the SHAKEN verification result. Further study is needed but could not be accomplished within the time frame of this report.

Before developing terminating service provider best practices for calls destined to enterprises, additional study is needed in the following areas: whether to transmit entire SIP Identity headers or other information such as RCD; current technical capabilities of enterprises and service providers; potential security issues; and whether the existing process of negotiating commercial agreements between service providers and enterprises is sufficient. Therefore, it is recommended that the FCC consider referring this further study to the CATA WG.

4. Glossary

Attestation – In the context of SHAKEN, the attestation of a call is represented by an “attest” claim allowing the OSP that is populating an Identity header to clearly indicate the information it can vouch for regarding the origination of the call. [ATIS-1000074] This includes the known validity of the TN-based caller identity.

Authentication – A process based on the Authentication Service (STI-AS) function defined in [ATIS-1000074] which is the SIP application server that creates an identity header [RFC8224] using private keys to generate a PASSporT [RFC8225] including a digital signature that protects the integrity of the information, most importantly the TN-based caller identity, used in a call.

Caller Identity (Caller ID) - The originating phone number included in call signaling used to identify the caller for call screening purposes. In some cases, this may be the Calling Line Identification or Public User Identity. [ATIS-1000082]

Certificate Validation – An act or process by which a certificate user established that the assertions made by a certificate can be trusted. [ATIS-1000084.v002]

Communication Resellers – Non-facilities-based VSPs that are wholesale Customers of and resell the voice services of facilities-based VSPs, whereby the facilities-based VSPs are also the OSPs for the reseller’s End-User subscribers.

Customer – Typically a service provider's subscriber, which may or not be the ultimate End-User of the telecommunications service.

End-User – The entity ultimately consuming the VoIP-based service and may include the End-User's device used for placing the call.

Enterprise – A business, non-governmental organization, or government entity that is a user of voice services. An enterprise may have direct relationships with any type of service provider, or service or TN reseller described in this document, and may have indirect relationships with any of these entities. An enterprise may initiate calls directly on its own behalf or may contract with other entities (e.g., call centers or hosted service providers) to initiate calls on its behalf. [ATIS-1000089]

FCC – Federal Communications Commission. The FCC may also be referred to in this document as "the Commission."

Form 499-A – An FCC multi-purpose form used for annual reporting revenues which are used as the basis for federal Fund assessments, funding of some administrative functions, sharing costs for some telephone service administration, and calculating regulatory fees; and one-time (with obligation to revise if information changes) designation of an agent for service of process, and fulfillment of obligations to register with the FCC by law.

Identity – Unless otherwise qualified, an identifier that unambiguously distinguishes an entity for authentication and other security and policy application purposes.

Identity owner – This is the user, subscribed to the controlling operator, who is currently assigned a specific E.164 phone number for call routing purposes. This E.164 number may be presented to a called party as the user's calling party identity. The identity owner can authorize other users or subscribers of controlling or non-controlling operators to also use the E.164 number as caller identity in phone calls made on the identity owner's behalf. [ATIS-1000072]

Identity service provider – An entity that verifies, maintains, manages, and may create and assign identity information of other entities. [ATIS-1000044]

Individual – An entity with a characteristic of being human.

Intermediate Service Provider – The term Intermediate Service Provider means any entity that carries or processes traffic that traverses or will traverse the PSTN at any point insofar as that entity neither originates nor terminates that traffic. 47 C.F.R. §64.1600(i)

IPES – Internet Protocol Enabled Service is telephone service a VoIP provider can establish with telephone number access that uses a partner company (IXC or CLEC) at a minimum to manage traffic from other TDM providers.

IPsec – a secure network-to-network protocol suite for encrypting IP packets creating a network tunnel. IPsec is a layer 3 network security scheme independent of application versus session-based application layer encryption like TLS used in SIP or DTLS used for Secure RTP (Real-Time Protocol)

Large Enterprise – See 'Enterprise'.

Neighbor Spoofing – With neighbor spoofing, no matter where the call originates, the information on the receiver's phone matches or closely matches the local area code and several digits (NPA-NXX) of the called party's phone number – which makes the consumer more likely to trust the call and answer.

Originating Service Provider (OSP) – The service provider that handles the outgoing calls from a customer at the point at which they are entering the public network. The OSP performs the STIR/SHAKEN Authentication function. The OSP may also serve in the role as TNSP, Resp Org, TN reseller and other roles. [ATIS-1000089]

Resp Org – A Responsible Organization is an entity authorized by the FCC to assign tollfree numbers to Customers. A Resp Org may also be a service provider, a TN Reseller as well as act in other roles. [ATIS-1000089]

SIP – Session Initiation Protocol is the foundational signaling protocol for creating, modifying, and terminating voice calls on internet protocol (IP) networks. [RFC3261]

Small Business – A business entity of less size or scale than a large enterprise, which may have direct and/or indirect subscriber relationships with one or more VSPs.

Snowshoe Spamming – Snowshoe spamming is a variation of neighbor spoofing that occurs when the information on the receiver's phone matches or closely matches the local area code and several digits (NPA-NXX) similar to the called party's phone number. Snowshoe spamming is a strategy where calls are propagated over several telephone numbers in low volume to avoid detection. The strategy is akin to how snowshoes spread the weight over a wide area to avoid sinking into the snow. Likewise, snowshoe spamming delivers its volume over a wide swath of telephone numbers to remain undetected.

Subscriber's Identity – This is the name, title, and authority of the subscriber agreement signatory.

TDM – "Time Division Multiplex" is an inter-switch transmission protocol that relies upon channelized data transmission synchronized between two endpoints. As used in this document the reference to "TDM" may also refer to other "Non-IP" data transmission protocols.

Telephone Identity – An identifier associated with the originator or a telephone call. In the context of the SHAKEN framework, this is a SIP identity (e.g., a SIP URI or a TEL URI) from which a telephone number can be derived. [ATIS-1000080]

Telephone Number Caller Identity – represents the telephone number used in a telephone call that is uniquely associated with a subscriber.

Telephone Number Service Provider (TNSP) – SP that has been formally assigned TNs by the national numbering authority (e.g., NANPA). A TNSP may assign a subset of its TNs to a business entity (i.e., TN Assignee), to be used as Caller Identification (ID) for calls originated by the business entity. TNSPs can also serve in the role as OSP or TSP. [ATIS-1000089]

Terminating Service Provider (TSP) – The VSP of the called party. The TSP performs the STIR/SHAKEN Verification function.

Third-Party Vetting Service – A service provided to a VSP by a third party for the purpose of vetting potential and current subscribers.

Third-Party TN Validation Service – A service provided to a VSP by a third party for the purpose of confirming the right-to-use of TNs for potential and current subscribers.

TN-based Caller Identity – The originating phone number included in call signaling used to identify the caller for call screening purposes. In some cases, this may be the Calling Line Identification or Public User Identity. In other cases, this may be a TN-based caller identity that is not associated directly with the calling line or account of the subscriber. [ATIS-1000088]

TN Reseller – The party who holds the right-to-use a TN and offers for resale the right-to-use that TN.

TN Right-to-Use/Authorization – When a party is appropriately assigned a TN, this is the right-to-use that TN; the assignment confers the right to the use of the numbering resource.

TN Validation – A process by which an indirect End-User's authorization to use a telephone number or set of telephone numbers is established and the process of providing that information to the VSP originating the call onto the telephone network through the use of existing and upcoming standardized secure mechanisms. TN Validation can be performed at the time the right-to-use of telephone numbers is established or throughout the life of the contract.

UUID – Universally Unique IDentifier. Also known as Globally Unique IDentifier (GUID). A UUID is 128 bits long and can guarantee uniqueness across space and time. A standard which defines the format and procedures for generating a UUID is IETF RFC 4122, "A Universally Unique IDentifier (UUID) URN Namespace."

Value-Added Service Provider (VASP) – Generally, a third-party provider supporting value-added services, for example including applications beyond the core voice calling services offered by a traditional VSP. In this document, it is used as a general term for VoIP and VoIP application providers that offer voice services without having direct interconnection with other VSPs utilizing wholesale providers for call origination and termination.

Verification – A process based on the Verification Service (STI-VS) function defined in [ATIS-1000074] which is the SIP application server that checks the validity of an identity header [RFC8224] using SHAKEN certificates to verify the digital signature contained in a PASSporT [RFC8225] and then the integrity of the information, most importantly the TN-based caller identity, used in a call.

verstat – Verification Status is a tel-URI parameter that communicates the result of the Verification from the Verification Service (STI-VS). Expected values are: "TN-Validation-Passed": The number passed the validation; "TN-Validation-Failed": The number failed the validation; or "No-TN-Validation": No number validation was performed. [3GPP TS 24.229]

Vetting – A process by which a customer's identity and operational legitimacy is confirmed by their service provider. Confirmation can be performed at the time service is established (initial confirmation of identity) or throughout the life of the service subscription or contract (ongoing confirmation such as evaluation of roboscores or traffic patterns indicative of abusive robocalling). TNs are not part of the vetting process; TNs are covered by the TN Validation process.

Vetted – The successfully verified result of a vetting activity.

Voice Service Provider (VSP) – The service provider whose network is interconnected to other service providers to both originate and terminate calls across the telephone network. The VSP is responsible for performing both STIR/SHAKEN Attestation functions when acting as the OSP and STIR/SHAKEN Verification functions when acting as the TSP [ATIS-1000089] a.k.a. Telephone Service Provider.

Wholesale Service Provider – A facilities-based VSP that acts as: an OSP for the End-User of a Reseller, an Intermediate Service Provider, or a gateway provider.