IMPLEMENTING KYC ON YOUR NETWORK OR COMMUNICATIONS PLATFORM

PRESENTED BY Numeracle Aegis Mobile

KNOW YOUR CUSTOMER: IDENTITY VERIFICATION AND MONITORING FOR COMMUNICATIONS IN SUPPORT OF THE CALL AUTHENTICATION FRAMEWORK

TOPICS TO BE COVERED

Why KYC?
Executing the Verification Expectations of Robocall Mitigation Plans

Complexities of Identifying down to the Calling Party brand
KYC to fill the Enterprise Attestation Gap

Implementing a Local Policy Identity Verification Solution

- Identifying your Attestation A, B, C policies
- Elevating the Enterprise to A-Level Attestation

Implementing KYC-based Identity Verification and Risk Mitigation
Vetting, validation, monitoring, and authentication toolset

Getting Started With KYC
Utilizing the Aegis Mobile / Numeracle KYC identity verification and monitoring platform

Why KYC?

Necessities for a “Know Your Customer” Framework to Establish Verified Communications Identity

KYC didn’t use to be associated with the telecommunications industry, but as service providers execute their Robocall Mitigation Plans and continue to extend STIR/SHAKEN deployment in support of the FCC, identifying every entity originating traffic on your network or platform with confidence is the new normal and expectation.

Jessica Rosenworcel

"What that means is when a call is being made, a carrier can tell that it really is the person who they say they are on the line."

Acting FCC Chairwoman Rosenworcel on the critical nature of implementing the caller ID authentication framework.

Both the FCC and FTC, in particular, have been very vocal about these emerging requirements. Over and over they have maintained it’s the carriers’ and service providers’ responsibility to monitor and ensure no illegal traffic is being facilitated across their networks or technology platforms. **Three waves of cease and desist letters*** have been sent to voice service providers, or “VSPs,” found to be facilitating bad actor traffic, and they will not be the last.

Identifying every entity communicating across your network can often be easier said than done. Today, there is a complicated relationship between the entity behind the call (also referred to as the calling party, brand, or enterprise), its outsourced contact center partners, number provisioners, and any other party involved in facilitating the call’s origination.

*Cease and Desist Letters:
https://www.fcc.gov/document/fcc-issues-robocall-cease-and-desist-letter-tellza
https://www.fcc.gov/document/fcc-issues-robocall-cease-and-desist-letters-six-voice-providers
https://www.fcc.gov/document/fcc-demands-two-companies-cease-and-desist-illegal-robocall-campaigns

In order to achieve a trusted level of oversight into each party touching the call, down to the calling party (brand, enterprise) itself, is to develop a KYC process to vet and validate the brand's identity and its authorized use of phone numbers.

This goes many layers beyond understanding the service providers' direct clients — the ones they maintain an actual contractual relationship with. This spans the depths of VSPs also needing to understand their clients' clients (and those clients' clients, and so forth) as well as any intermediary who the service provider is directly or indirectly delivering or facilitating calls on or on behalf of, from the calls' origination to the calls' termination.

KYC fulfills service provider requirements as defined by the FCC:

- The need to vet and validate the identity of entities using the network
- Authentication of brand identity + authorization to use phone numbers
- Implementing a local policy to identify and monitor for bad actor traffic

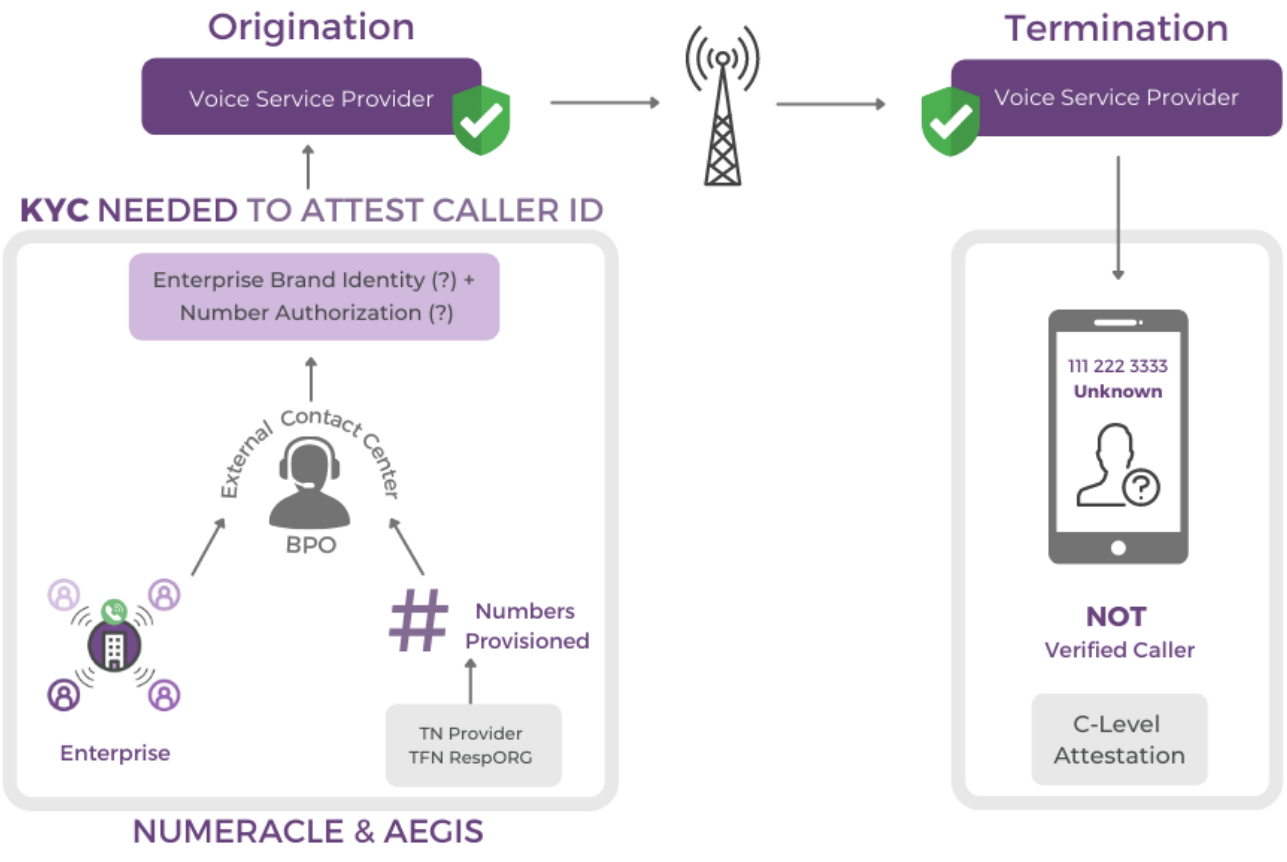
Complexities of Identifying down to the Calling Party brand

STIR/SHAKEN Framework: C-Level Attestation

A very common and complex situation faced by many originating service providers is the role of the intermediary in delivering traffic on behalf of an enterprise brand. In this situation, a Voice Service Provider (VSP) is originating calls that are facilitated through a Business Process Outsourcer (BPO) or external contact center on behalf of its enterprise clients.

In this case, the VSP has a direct contractual relationship with the external contact center, but not the enterprise brand itself. To further complicate things, the VSP also doesn't have direct visibility into the source of phone numbers procured for use by the enterprise brand. It's perfectly plausible that the VSP has no idea who the enterprise brand actually is. Therefore, how could this VSP be able to attest to the identity of the caller and its authorized use of the phone numbers it intends to display?

Figure 4. Attestation Level C for Enterprise



Complexities of Identifying down to the Calling Party brand

STIR/SHAKEN Framework: C-Level Attestation

This situation results in the terminating service provider's receipt of a C-Level STIR/SHAKEN attested call, an enterprise brand who is probably unhappy with the inability to achieve A-Level attestation, and an originating service provider who's looking for a solution to be able to verify, with confidence, down to the brand identity.

There is still value in C-Level attestation as it relates to traceback efforts, but the value to both the caller and the callee is diminished as the call will not be delivered with A-Level-defined verified number indicators (such as a checkmark, etc.).

Implementing a Local Policy Identity Verification Solution

Identifying your Attestation A, B, C policies

For originating service providers, your "local policy" otherwise known as "how you define how to meet the requirements of signing to A, B or C level based on the STIR/SHAKEN standards" starts with the question of "how deep do you want to vet?" Is a signed contract in hand good enough to stand up to the robust expectations of the FCC, or does it need to go deeper?

As explored in the section prior, "Complexities of Identifying down to the Calling Party brand," what if your direct (contractual) customer is not the calling party? Can you trust your direct customers' processes to vet their customers one level down, or is that additional level of KYC vetting and validation required based on how you define your local policy?

Based on the Standards, it's expected when an originating provider signs a call at A Level, that provider knows who the actual calling party is using that phone number; this requires a KYC process that must extend all the way down to the caller identity of the brand or entity represented within the body of the call.

As a VSP, you need the confidence to trust the users of your platform all the way down to the brand level. Any resistance you see from customers on your platform who don't want to meet the requirements of your local policy and demand to remain anonymous might just be the bad actors you don't want to unknowingly facilitate a la Globex or Alcazar.

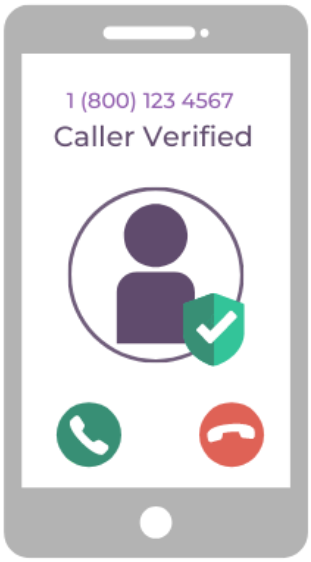
Elevating the Enterprise to A-Level Attestation

The industry has done a pretty good job at spreading the word about A-Level Attestation, so much so that enterprise brands are asking for it directly without even truly grasping what it means from a technology perspective.

So when it comes to your customers asking you for A Level Attestation, you need to do your part to know whom the calling party brand represented within the call is, regardless of whether or not they procured numbers from you or are directly contracted with you.

To elevate enterprises you're currently attesting at B or C-Level to A-Level, a KYC process has to be implemented to authenticate each intermediary along the call chain down to the calling party brand in order to fulfill the due diligence requirements as set forth by the FCC.

Outbound calling structure involving multiple entities in the call scenario makes achieving a STIR/SHAKEN A-Level attestation for an enterprise brand that outsources calling operations to communications vendors (even the 100% legal, compliant, and trustworthy vendors) extremely cumbersome and difficult. That is Aegis Mobile and Numeracle have teamed up to make the process a whole lot less complicated.



Implementation of a KYC-based local policy solution supports service and platform provider's ability to assess the level of attestation achievable based on the availability of information to vet and verify down to the enterprise or calling party brand, with confidence.

Implementing KYC-based Identity Verification and Risk Mitigation

A comprehensive vetting, validation, monitoring, and authentication tool set

Aegis Mobile and Numeracle have joined together to support the ongoing service provider requirements of STIR/SHAKEN execution and the associated Robocall Mitigation Plans required to continue to strengthen and ensure the success of the caller authentication framework deployed.

The implementation of a KYC process in communications is all about bringing identity into the voice network so the consumer being called knows the entity calling them has been verified. The Aegis + Numeracle KYC-based identity verification and risk mitigation solution allows the service provider to use company information collected to unambiguously identify via research of the business entity to determine trust level and corresponding service level in order to support these verification requirements, regardless of a direct relationship to the calling party brand, or not.

This solution was designed for:

- Service Providers fulfilling **Robocall Mitigation Plan** surveillance, risk monitoring, and fraud detection requirements
- Service Providers elevating enterprise calls from C or B-Level attestation to **A-Level**
- The need to implement multi-tiered levels of **entity identification** to cover the various intermediary touchpoints a call passes through (vendors, contact centers, etc.), all the way down to the brand level
- Avoiding the mistakes of other VSPs found to be facilitating illegal calling activity due to **lack of KYC process in place**

Whatever your local policy determines as the fulfillment of the verification requirements outlined by the FCC or in reaction to FTC orders against VSPs found to be facilitating illegal activity, we can help you meet those verification checkpoints. However you'd like to define your KYC process, completion of identity vetting and phone number authorization, implementation of double-authenticated touchpoints, collection of documentation to explain the needs of the call down to the brand level, etc., Numeracle and Aegis are here to provide a flexible, fully-auditable solution to meet your needs.

Getting Started with KYC

Utilizing the Aegis Mobile / Numeracle KYC identity verification and monitoring platform

To begin the process of instituting a KYC-based entity vetting process within your organization today, contact us at www.numeracle.com/contact and mention Aegis or connect directly with Aegis at https://aegismobile.com/contact/ and mention Numeracle.

Numeracle

Numeracle's Entity Identity Management™ Platform and Verified Identity™ platform enable legal entities to prepare for STIR/SHAKEN, prevent improper call blocking and 'Fraud' labeling, and employ best practices to prevent 'Spam' labeling by working with tech providers, carriers, device manufacturers, & analytics companies, providing visibility and brand management across the telecom ecosystem.

Aegis Mobile

Aegis has been a trusted channel "verification" partner for wireless carriers, aggregators, & enterprise businesses for over 14 years. Aegis began working with the largest U.S. wireless carriers to provide verification & compliance services that ensure the safe & beneficial growth of the digital content market for mobile consumers through robust proprietary tools and multiple automated platforms.