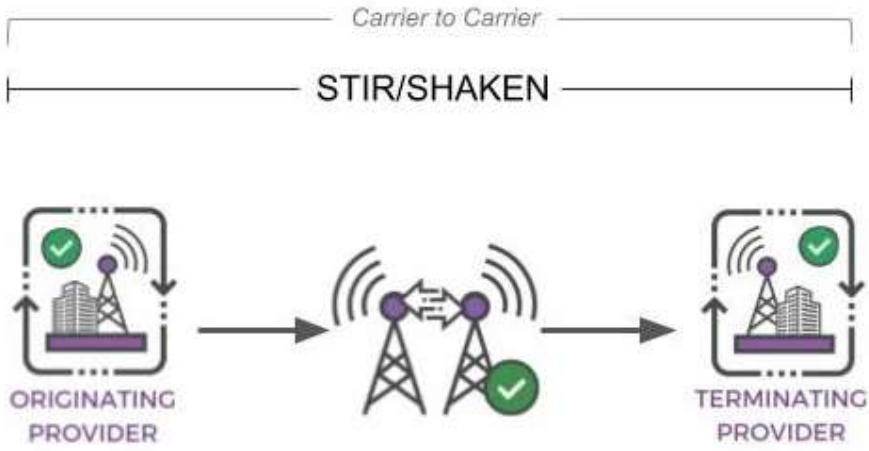
Numeracle

About Numeracle

Numeracle, Inc., is the industry pioneer and leader in verifying the identities of entities placing legal outbound communications and ensuring that verified identity information is transmitted securely to the communication's recipient. While thus far Numeracle's operations have been solely in the United States and Canada, we want to share our experiences as to what is working and what is not so that other countries can benefit from early efforts in the United States.

Numeracle was founded in 2018 in the United States in response to the threat posed to lawful communications by the efforts to combat illegal and unwanted robocalls. Numeracle's founder and CEO, Rebekah Johnson, foresaw that legal and wanted calls, such as reminders from the pharmacy that a prescription is ready, a callback in response to an online inquiry about a product, or a call from a telecom service provider that the repair technician had been dispatched, could be caught up in the efforts to block and label illegal and unwanted mass outbound communications. In 2016, she was asked to join the Federal Communications Commission's Robocall Strike Force because of her expertise working with legal outbound callers. She was also invited to join the FCC's Hospital Robocall Protection Group to assist hospitals in combating inbound illegal robocalls that disrupted hospital operations. Ms. Johnson is a Board Member of the Alliance for Telecommunications Industry Solutions (ATIS), a global standards organization for the telecommunications industry. She is also a member of the STI-GA's External Feedback Forum, a group chartered to inform the STIR/SHAKEN governance authority about the effectiveness of STIR/SHAKEN.

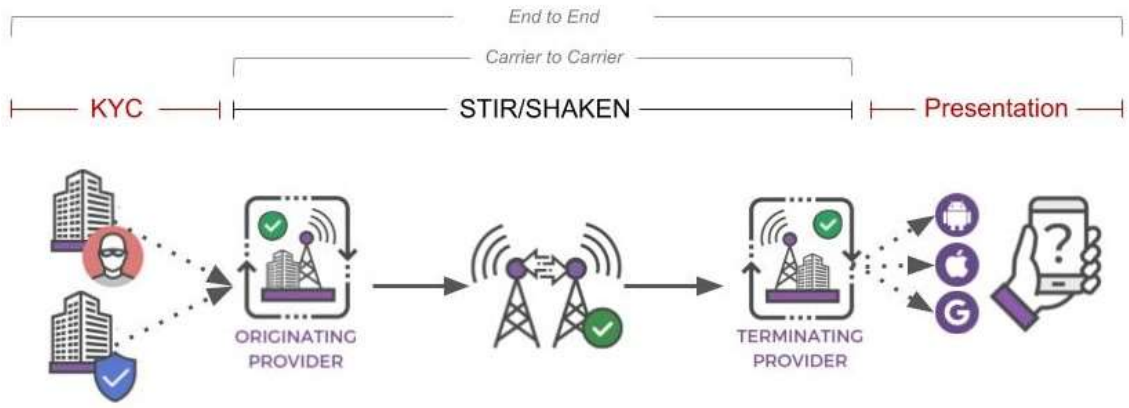
Numeracle recognized the value of STIR/SHAKEN as a core technology in fighting robocalls but thought it did not go far enough. STIR/SHAKEN, and its UK equivalent of Caller Line Identification, is designed to transmit the identity of the originating service provider and what it knows about whether the caller has the right to use the displayed phone number to the terminating service provider. That's it. It does not include the identity of the calling party, nor is there any guarantee that the verified information makes its way to the device of the call recipient.



Numeracle has made several advances beyond the base STIR/SHAKEN framework to further the goal of end-to-end verified identified communications. Ms. Johnson introduced the concept of Know Your Customer ("KYC") to the telecommunications industry in the United

States in 2017 and 2018 through a series of working groups she hosted to work with carriers and analytics engines ("AE") to ensure that legal communications were not adversely affected by anti-robocall efforts. Other industry participants recognized the value of verifying the identity of call originators, and KYC concepts have become a core part of the global effort to combat illegal robocalls. The Federal Communications Commission has mandated that voice service providers enact and follow KYC policies for both their call origination customers and upstream service providers.

Numeracle believes the best way to fight illegal robocalls, including illegally spoofed calls, is to identify those entities making legal calls and to transmit the verification of that identity end-to-end and present the information to the recipient of the call. If the communications ecosystem identifies the legal and wanted calls, it can then focus anti-robocall efforts on those callers who are unwilling or unable to identify themselves.



Our collective efforts here are ultimately to protect consumers, who do not care about which originating service provider placed the call. What consumers want to know is that the name on their incoming call screen is who it purports to be. The efforts of industry and regulators should be to develop the regulatory framework and implement the technology that makes that happen. The individual tools, such as traceback, CLI, STIR/SHAKEN, KYC, and others are merely tools that enable the verification, transmission, and display of identity to the recipient of the communication.

Numeracle is grateful that Ofcom's Objective 2 in Section 2.10 recognizes the need to support legitimate phone calls. Anti-robocall efforts in the United States have often failed to recognize the importance of this objective. It is simple to block 100 percent of fraudulent calls by blocking all calls. Numeracle believes that the balance in the United States has been too far in favour of blocking or labelling legitimate calls out of fear of not blocking or labelling all the bad calls.

3.1

We must not lose sight of the fact that the goal is to eliminate fraudulent calls. Not all fraudulent calls are spoofed, and not all spoofed calls are fraudulent. Ofcom's goal should be to

eliminate scam calls and to empower consumers to accept, avoid, or block legal but potentially nuisance calls by clearly displaying the verified identity of the caller.[1] Cracking down on number spoofing is one means of accomplishing this goal, but ultimately the mission should be to verify the identity of the caller and not the telephone number ("TN") used by the call originator. Even without the additional confusion of spoofing, TNs change but callers endure.

Scam calls in the United States typically utilize one of three strategies: 1) number spreading (sometimes called snowshoeing) or utilizing a large number of legitimate phone numbers to avoid detection by call filtering algorithms and minimize traffic spikes[2], 2) spoofing random phone numbers or phone numbers with the same area code as the call recipient but without attempting to impersonate any single individual or organization, and 3) spoofing attempts of a specific legitimate number in an impersonation attempt.

Not all spoofing is bad. In the United States, it is a common practice for a communicating entity to spoof the same outbound number across multiple call centres potentially using multiple carriers to have a unified callback number. There are other legitimate uses of spoofing as well. One example is that a pharmacy chain may hire a call centre to place automated calls that prescription medications are ready for pickup. The caller spoofs the number of the individual store location where the call recipient should pick up their medication so that if the customer has a question, he or she can call the local store and not the centralized system that originated the call. Similarly, doctors and other professionals may spoof their office TN from their mobile phones so that return calls go to the business phone and not to their personal cell phone. Efforts to combat illegal spoofing should recognize these legitimate uses of spoofing.

4.1

Ofcom's proposal is, at its core, to implement STIR/SHAKEN as has been done in the United States. While CLI is an essential ingredient in solving scam calls propagated by number spoofing, on its own it falls short. CLI is a means of identifying the originating carrier. What

[1] One oversight that has thwarted progress on fighting illegal and unwanted robocalls in the United States is the failure to reach consensus on the definitions of those terms. While "illegal robocall" may seem self-explanatory, it is not. Impersonation scams are clearly illegal. But there are grey areas about marketing calls made without consent in violation of the U.S. telemarketing laws. The carriers and the AEs blocking and labelling these calls cannot know the legality of the call as they are unaware of whether the call recipient has consented, and the lawfulness of the call hinges on consent. Furthermore, "unwanted" has never been defined, and perhaps it cannot be defined. Political calls, surveys, and charity calls in the United States are exempt from some calling regulations. Are they wanted? Who knows—and certainly the carriers and AEs do not know with any certainty as to any individual call recipient. Calls made by debt collectors are another fuzzy area of "unwanted." Some consumers want to know if they have unpaid debt and want to receive calls about a debt to resolve the matter, while others evade such calls as they have no intention of paying the debt. Are these calls unwanted? Should they be blocked or labelled as unwanted? Reasonable minds may differ. Similarly, Ofcom's efforts to fight "nuisance" calls will fail without a consensus about the meaning of "nuisance" and how it can be defined without regard to individual consumer preferences and the inability of telecom providers to know the content of any individual call.

[2] Often the use of large numbers of legitimate phone numbers is combined with cycling phone numbers in and out of use to further avoid detection.

we need to do, however, is identify the caller. Identifying the originating carrier is a means to an end, but not the end in itself.

A phone number is not a permanent unique identifier. Ofcom should encourage the adoption of a permanent unique identifier for organisations and entities placing large volumes of calls. Fortunately, the hard work in this space has been done by the Global Legal Entity Identifier Foundation (GLEIF), which is a Not-For-Profit organisation established by the Financial Stability Board of the G20. GLEIF arose out of the 2008 crisis in the financial industry as a means of combatting fraud in international monetary transactions.

GLEIF created a process for verifying the identity of entities such as businesses, non-profits, NGOs, governmental agencies, and the like. Each entity is assigned a globally unique ID that it can then use in transactions to show that the entity is who it purports to be and that the individual claiming to represent the entity is authorized to do so. Numeracle is working to incorporate the Legal Entity Identifier (LEI) framework overseen by GLEIF into voice call signalling to transmit a secure version of the LEI ID known as a Verifiable LEI (vLEI) to the call recipient. Numeracle's CEO recently participated in a panel discussion at a Mobile Ecosystem Forum event in London about how entity and organizational identities can be used to combat fraud in communications. https://youtu.be/Qcoqugi0HuQ. GLEIF CEO Stephan Wolf also participated in the discussion.

Numeracle cautions that the United Kingdom should not proceed down the same paths taken in the United States that have been ineffective at best and harmful at worst. Illegal robocalls remain a widespread problem here, and the best available data shows little to no decrease in illegal calls since the FCC mandated the implementation of STIR/SHAKEN two years ago. And the problem of legal, wanted calls being inaccurately labelled as "Spam" continues to grow.

The core of the U.S. fight against illegal robocalls since 2016 has been the use of analytics engines ("AE") to attempt to identify illegal and unwanted calls through big data analysis, with a focus on number spoofing.[3] This attempt has failed miserably. When the AEs began operations in the mid to late 2010s, the predominant robocall pattern in the United States was large-scale use of a single telephone number or a small number of TNs to place the outbound calls. The AEs developed their algorithms to identify these traffic spikes and to block or label them. But since these algorithms were developed, the illegal callers have adapted and now generally spread their calls out with illegal spoofing and, increasingly, the use of large groups of non-spoofed phone numbers to use each displayed outbound phone number a single time or a small number of times. Large traffic spikes on a single calling number are not necessarily indicative of illegal calls. In fact the opposite is true as illegal callers increasingly spread their traffic across many numbers and several providers, but the AEs continue to flag calls made by Numeracle's clients making lawful communications if their traffic patterns somehow offend the presumptions about permissible calling patterns made by the AE algorithm creators. The AEs need more and better information than what is currently

[3] While STIR/SHAKEN is supposedly part of the dataset used by the AEs, many calls from legitimate businesses remain unsigned because of exemptions and gaps in the IP network. Whether a call is signed or not signed, and the level of attestation, has very little relationship to the legality of a call. Furthermore, even within some of the largest mobile carriers, the AE vendors are not also the STIR/SHAKEN authentication and verification vendors and there has been limited integration of STIR/SHAKEN information into AE analysis.

available from call signalling alone, authenticated or otherwise. Better, more focused, authenticated information about legitimate callers can be made available but it requires an industry effort to decide what information obtained from KYC efforts should be encoded, authenticated, and transmitted to AEs such that their algorithms can be significantly more accurate and efficient.

Five years ago, Numeracle pushed for a number registration, monitoring, and remediation process for legal callers to work with the AEs in an attempt to prevent inaccurate labelling and blocking of legal calls. All three major AEs in the United States adopted policies implementing this three-part process. Step one: The AEs permit legal callers to register their numbers for free in hopes of preventing spam tagging and blocking by giving the AEs knowledge about their identity and calling practices. Step two: Monitoring of the reputation scoring by the AEs. Step three: Remediation of inaccurately labelled or blocked numbers. Unfortunately, step two does not always come free of charge in the United States. Numeracle noticed a 98% decrease in spam tagging for its customers with one AE after Numeracle began paying for monitoring of its customers reputation scores rather than just relying on the AE's free registration and remediation process.

Equally troubling are the systems controlling the deployment of branded calling services in the United States—sold by the very companies whose inaccurate spam labelling and blocking has led to the need for legal callers to try all possible means to get their communications to their customers without being labelled or blocked as spam. Companies who are frustrated with inaccurate labelling, blocking, or just decreased answer rates in general are willing to pay terminating carriers to properly display their name and, in some cases, their logo to call recipients. While the AEs do not guarantee that paying for branded call display overrides spam labelling, the KYC policies in place to purchase branded calling in the first place provide the very information the AEs need to confirm that the caller is not making illegal calls. The fox is guarding the henhouse. In the United States, the AEs are unregulated and unresponsive to any demands other than those of their carrier partner. The UK should be wary of increasing the role and power of the AEs without imposing tight restraints on their actions with a free, effective registration and remediation process for legal callers.

Branded calling has value as the launchpad for a superior call delivery system that incorporates CLI at its core but extends the system at both ends. At the originating end of the call, the process should not begin with the originating service provider. The OSP should have a careful KYC process in place, and the OSP should embed the caller's identity into the call signalling. Technologies and standards to do this already exist and implementation is just around the corner in the United States. At the terminating end, the CLI information should not just be viewed by the terminating service provider and its AE partner. Instead, the caller's name and, optionally, its logo should be presented to the call recipient with an indicator that the information has been verified and transmitted securely.

The comments at 4.43 regarding technical limitations of blocklists such as Do Not Originate (DNO) lists are well considered. It is worth noting that current implementations of STIR/SHAKEN are dependent on the use of X.509 security certificates as the source of the identity of the entity signing the call, and that management of Certificate Revocation Lists (CRLs) in web Public Key Infrastructures (PKIs) has proven problematic with regard to developing and enforcing policy for revocation, vulnerability to DoS attacks, and growing too large too quickly leading to alternatives such as On-line Certificate Status Protocol (OCSP)

and “delta CRLs”. These operational concerns have yet to be a significant issue in the nascent implementations of STIR/SHAKEN, but broader adoption of call authentication, both by additional service provider entities and non-service provider entities for use cases such as mutual authentication, requires careful consideration.

With regard to international adoption of STIR/SHAKEN, there is a risk that adoption will be severely curtailed by problems with interoperability if each jurisdiction makes changes to the protocol requirements or the governance and policy administration that conflict with policy and technical choices made in other jurisdictions. For example, the Certification Authorities (CAs) that issue X.509 security certificates to service providers in one jurisdiction may not be trusted by service providers in another jurisdiction. This problem of “rogue CAs” has been an issue for the web PKIs and led to the creation of the CA/Browser Forum but which has only regional influence. Regional implementation also implies complex gateway configurations to support interoperability between regions.

5.1

Ofcom’s basic structure for CLI is sound. Many of the implementation and technical difficulties have already been worked out abroad in countries with earlier deadlines for implementing similar systems. And the UK will have the advantage of an all-IP network in which to deploy CLI. Antiquated network infrastructure in the United States that still uses TDM technology has thwarted ubiquitous STIR/SHAKEN implementation. Due to complicated call routing systems, many signed calls that are destined for a STIR/SHAKEN compliant terminating provider nevertheless have the authentication information dropped due to a non-compliant carrier somewhere in the call path.

Many originating providers will always be unable to attest to the accuracy of caller ID information. As a result, Ofcom’s suggestion that calls arriving without the highest levels of attestation may be used by terminating providers as grounds for blocking calls will result in legitimate calls being blocked by terminating providers.

There are numerous complaints in the US that “attestation” is unreliable. Making it reliable is non-trivial because it is difficult for a service provider to be confident in all use cases that the caller has authoritative right-to-use of the telephone number being presented. The most common example discussed is the case of a multi-homed enterprise where it may originate a call using telephone numbers from service provider A on trunk groups connected to service provider B, and vice-versa. This multi-homed enterprise problem was the genesis for the Technical Report from the Alliance for Telecommunications Industry Solutions (ATIS) titled "Study of Full Attestation Alternatives for Enterprises and Business Entities with Multi-Homing and Other Arrangements."

There is a dangerous assumption that calls that fail verification can be assumed safe to block. This is a dangerous assumption because signed calls in the US routinely fail verification for ordinary operational reasons. The most common reasons for verification failures are “number normalization” in intermediate networks, and problems with an expired or new certificate.

Number normalization occurs as an ordinary course of business to re-format numbers for the purposes of call routing. The routing logic or other functional logic expects a particular format such as E.164, or not, and the network edge components will frequently re-format

calling and called numbers on ingress to a format used by the routing or other function application server. A failure to re-format the re-formatted number back to the original format on egress frequently causes the call to fail verification. In addition to "number normalization", routing translations required for call forwarding, agent transfer, or Toll Free termination often result in changes to the destination telephone number that will cause a call to fail verification.[4]

A call signed with a reference to an expired certificate should always fail verification. A call signed with a reference to a new, but unvalidated certificate can take several seconds for the data to be downloaded, the certificate path calculated, validated and cached, and the public key of the end-entity certificate used to verify a call signature. In a busy network receiving tens of thousands per calls per second during busy hours, it is not prudent to wait for new certificate to be downloaded, validated, and to verify the call signature. In fact, doing so would represent a very effective vector for a Telephony Denial of Service (TDoS) attack. Instead, calls should be permitted to complete unverified. Greater consideration should be given to an "unverified" audio or visual indication to the called subscriber. Ofcom should consider potential impacts of this proposed blocking measure from TDoS attacks on verification, and on public safety emergency services, and government emergency telephone services.

This concern is not just hypothetical. A personal friend of the author had a mobile phone on one of the three major wireless providers in the United States, and her husband had a phone on another of the three major providers. A certificate for the husband's originating carrier had expired, and the terminating carrier blocked a call from husband to wife at the network level because of the expired certificate—even though their phone numbers were in each other's contacts. This happened during a family emergency.

5.2

CLI authentication as envisioned by Ofcom is unlikely to materially reduce scams and unwanted calls. The primary effect will only perhaps change the tactics of scammers. Despite the implementation of similar CLI authentication measures in the United States, scam call volumes are constant and perhaps even rising.

Ofcom should refocus its efforts not on stopping all improper spoofing, an impossible task given the structural limitations inherent to originating service providers' ability to attest calls, but instead focus on authenticating and displaying the identity of the caller. Even if consumers were able to fully trust the accuracy of the CLI presentation of the calling phone number, most consumers do not memorize individual phone numbers. Unless a number is a

[4] The STIR standards include a special kind of call authentication that uses additional signatures to account for the routing translations. The translated telephone number(s) is included in a "div" (an abbreviation for diversion) Personal Assertion Token (PASSporT). Complex calling use cases may change the destination telephone number more than once. The additional "div" PASSporTs can cause a SIP INVITE to grow quite large jeopardizing the call signaling at layer 4 where fragmentation and re-assembly of a User Datagram Protocol (UDP) encapsulated SIP message can cause the SIP INVITE to be dropped. Service provider support for use of "div" for complex call scenarios is not widely adopted within the US and partially because not all STIR/SHAKEN architectures use the ATIS-1000074 reference architecture and instead apply signatures and verification at edge elements (often a Session Border Controller) and the original SHAKEN PASSporT is stripped by the Verification Server and lost on ingress to the network.

presaved contact, call recipients will remain unable to know or trust the identity of the calling party and scam callers will be able to exploit this lack of knowledge to pursue scams. Ofcom should encourage the development of verifying callers' identities and some subset of real-world trust attributes and presenting the name—not just the phone number—to the call recipient.

Service providers should be required to implement specific KYC processes and procedures in order to ensure that a reasonable standard of care is being taken to validate the identity of both service provider and non-service-provider customers, review customer history and call intent, and monitor ongoing activity. Numeracle has released a template for service provider KYC policy for providers to use as a standard. https://www.fcc.gov/ecfs/document/1042778647719/2[5]

Ofcom should pursue standards for authenticating the identity of calling parties, especially the identities of legitimate robocallers, and requiring service providers to transmit these authenticated identifiers to the call recipient. Such a system could be scaled and standardized considerably by authorizing non-service provider registration agents to work either directly with callers or in conjunction with service providers to authenticate callers via a standard process. Registration agents could be overseen by Ofcom or an authorized industry body to ensure appropriate actions are taken.

6.1

Ofcom should ensure there are clear standards for when calls may be labeled or blocked by terminating providers with clear systems for an evidentiary standard required in order to block and label. Additionally, Ofcom should require a widely available and prompt system of redress in cases of improper blocking and labeling. Service providers should be held directly accountable for improper blocking and labeling, regardless of whether the blocking and labeling was done by the service provider or the service provider's AE vendor partner. AEs in the United States callously ignore the real difficulties that businesses face in placing voice communications that are blocked or labeled as "spam" or "potential spam." The AEs argue that inaccurate labeling is not important because their systems allow the calls to go to voicemail, such that even an unanswered call labeled as spam still allows the caller to get a message through to the recipient.

The negative impact of negative spam labeling is proven by the AEs themselves as they sell branded calling products that claim to alleviate the harms caused by the AE's own spam labeling: Hiya sells branded calling as Hiya Connect and notes that "Businesses often look to static caller registries to avoid and resolve inaccurate spam labels."[6] What Hiya does not say is that for one-third of the consumer voice market in the United States, Hiya is the one doing the inaccurate labeling! Similarly, Hiya's competitor Transaction Network Services (TNS) also sells branded calling as a solution to inaccurate spam labeling that TNS is itself doing:

[5] An editable Word document version of the Numeracle Model Standards for KYC is available at https://www.numeracle.com/kyc-policy-guide.
[6] https://www.hiya.com/products/connect

"Enterprise Branded Calling controls spam labeling and helps increase answer rates for legitimate callers that follow best practices, enhancing overall enterprise calling reputations and boosting your business."[7]

6.2

One strong point of the U.S. efforts against illegal robocalls has been the success of the Industry Traceback Group (ITG). The ITG began as an informal and voluntary industry working group of concerned providers. It often ran into non-participating providers who declined to reveal the source of illegal calls that had traversed or originated on their networks. In 2019, Congress passed the TRACED Act that permitted the FCC to approve a mandatory traceback process. Even with the gaps in STIR/SHAKEN, the ITG has proven to be remarkably effective at identifying the source of illegal robocalls.

Properly implemented and with universal service provider compliance, CLI will largely eliminate the need for a carrier-by-carrier traceback process such as that currently managed by the ITG because the originating service provider's identity will be embedded in the call signaling. But the effectiveness of tracing back to the caller and not just the OSP depends on requiring an effective KYC process and enforcing non-compliance so that when a call is traced to the OSP, it can identify the offending customer to enforcement agencies and provide sufficient information to investigate the appropriate calling party.

The shortcomings of the CLI process Ofcom is planning are revealed with the following problems: How will Ofcom prevent scam callers from obtaining new services with another service provider? How will Ofcom prevent scam callers from circumventing any such restrictions or enforcement placed on individuals or legal entities simply by setting up a new legal entity under a different name? As stated above, Numeracle believes the ultimate solution to scam and illegal calls is to require the identification of the entity placing the call and embedding that information in the call signaling for transmission to the call recipient.

7.2

Ofcom's proposed CLI Authentication Administrator body should have representation from groups other than service providers, for two reasons. First, as Ofcom stated, "It is important to agree and define a robust approach to how the 'trust service' for digital certificates would be designed, as this is complex to set up and requires a constant level of maintenance by skilled practitioners." Many of the most skilled practitioners necessary to contemplate the complexity of a CLI authentication program are found outside of service provider organizations. Many service providers in the United States utilize non-service provider vendors for technical elements of certification, something that is highly desirable to improve the efficiency and adoption of any framework. The participation of such experts would improve the knowledge and effectiveness of the Administrator.

The decisions reached by the Administrator regarding the standards of trust and identity have direct and important implications for calling businesses and consumers. The Administrator would be best able to enact policies and procedures that are achievable by callers and valuable to consumers by incorporating direct representation from these groups.

[7] https://tnsi.com/enterprise-branded-calling/

Second, Ofcom should consider the creation of a separate entity or sub-entity within the Administrator to establish KYC policies and procedures related to the identification and transmission of verified information about calling parties. Such an entity should have heavy representation from non-service provider enterprises, consumers, and experts in the field of identity verification. Telecom service providers generally do not employ individuals with expertise in scalable and trustworthy systems of business and consumer identity validation and transmission, so Ofcom should encourage cross-collaboration with identity experts in the telecommunications, financial services, and digital identity spaces, such as GLEIF as discussed above.

7.3

A centralized numbering database would be a useful adjunct to the CLI framework but may not be feasible or worth the expense. Numbers are currently assigned, reassigned, ported, and resold across the globe in a manner with little to no oversight in many countries. While this system has advantages in speed and flexibility, the disadvantage of lack of transparency is glaring.

Creating a database to understand fully the reseller relationships and assignments of each phone number would likely be difficult and costly to implement and would not directly impact the fundamental issue and desire of consumers—giving call recipients the ability to understand the verified identity of the calling party behind the phone number. Ofcom could better apply limited resources by investing in the establishment of standards for more reliable calling party identifiers beyond the phone number and the display of verified calling party identification to the call recipient.