BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

In the Matter of	)	
	)	WC Docket No. 17-97
Call Authentication Trust Anchor	)	
	)	FCC 17-89
	)	

Comments of Noble Systems Corporation

Filed August 14, 2017

Karl Koster, Esq.
Chief Intellectual and Regulatory Counsel
Noble Systems Corporation
1200 Ashwood Parkway
Atlanta, GA 30338

I. The Commission Should Focus on the Long Term Technology Solution

Noble Systems believe that the Shaken and Stir ("S&S") technology approach is the long term solution for combating illegal calls. This technology is application for a variety of illegal call types, as it is not dependent on blocking a particular type of calling party number. This technology can also be used as the basis for reducing unwanted legal calls and can be used as a criteria for call blocking. Shaken and Stir has the potential to facilitate identification of where a call was authenticated, and the goal is that this function should be performed as soon when a service provider receives the call.

Those originating illegal calls continue to do so despite various laws because of the anonymity offered by using inexpensive VoIP-based technology. S&S offers the promise of being able to quickly identify where a call was authenticated and thus allows the veil of anonymity of the calling party to be at least partially removed. In theory, a scammer originating an illegal call could be reported to law enforcement. This would allow easy identification of the authenticating network; potentially the call originator could be identified quickly. Service providers authenticating such calls, once notified by an agency or legal authority of potential illegal activity, would likely quickly investigate whether their subscriber is engaged in activities violating their terms of service with that service provider. Law enforcement would have information allowing them to act quicker. Although S&S can be used as a criteria for blocking call that has not been authenticated, the effectiveness of S&S in the long term is based on providing transparency as to the point of call authentication, which in many cases facilitates identification of the call originator.

However, the Commission has been entertaining a number of other proposals based on call blocking using various types of "blacklists," which Noble Systems characterizes as types of service-specific database solutions. These solutions may be used to outright block a call or otherwise 'label' a call, e.g., label it as being "spam" or "nuisance." The Commission has entertained proposals allowing carriers to establish, e.g., a database for unassigned numbers, unauthorized numbers, or unallocated numbers, which is checked as a basis to block or label a call by a carrier, hence the so-called "blacklist" nomenclature. Many of these database solutions can be implemented solely within a carrier (intra-carrier) or implemented with the involvement of multiple carriers (inter-carrier). For example, an intra-carrier database of a carrier's own

unassigned numbers could be used to block any call handled by that carrier indicating an unassigned number. However, the effectiveness of an intra-carrier solution is limited, and hence the Commission is investigating inter-carrier service-specific solutions, such as a national, unassigned number database, which all carriers would update and access in real-time.

There are two important aspects that the Commission should recognize regarding S&S and these blacklist service-specific database solutions. First, these service-specific database solutions are inherently ineffective, even for the short term. After spending time, money, and resources to build and deploy a database to identify calls using unassigned, unallocated, or unauthorized calling party numbers, scammers will simply alter their calls to use valid calling party numbers. This is already being done, and has the potential for blocking or mislabeling telephone numbers from legitimate callers.[1] Scammers using the "neighbor spoofing" technique today render the unassigned, unallocated, and unauthorized service specific databases obsolete before they are even available. The long term solution is to remove the anonymity of the call originators by authenticating calls. Eventually, identifying where the call is authenticated will facilitate identify the entity originating the call.

The ineffectiveness of using a blacklist approach can be illustrated with an example that unfortunately happens all too often now. A school emergency leads to a mass calling effort to all the telephone numbers of the children's parents. From a call blocking analytics perspective, the sudden origination of a large number of calls using a single calling party number may lead to those calls being treated by a carrier as "robocalls." The danger to blocking or mislabeling such calls to the parents as "spam" in an emergency is unthinkable.

The potential for such errors leads to the suggestion of another proposal, which is just as ineffective, and that solution is to use a whitelist to counteract the possibility of numbers being blacklisted. Using the above example, the school's number could be added to the whitelist. But, this is approach is ineffective because scammers will now know that by spoofing the school's

[1] The author made an ad-hoc check to a few numbers listed in the FTC's robocall complaint database for August 10, 2017. One of those numbers alleged to have originated a robocall for medications/prescriptions was that of a county board of commissioners in the state of Georgia. Presumably, the scammer spoofed this number.

number, their calls will not be blocked. This "whack-a-mole" approach is not an effective long term solution.

The second aspect the Commission should recognize is that to the extent industry and regulatory resources are directed to developing such service-specific databases, it will detract from developing the long term approach. The industry does not have unlimited resources. It is unrealistic to expect industry to spend time and money to deploy inter-carrier databases for unassigned/unallocated/unauthorized numbers and simultaneously deploy S&S technology. The Commission should focus on a single solution, which is the S&S approach, that is more effective.

The Commission has already received comments advocating against any mandates for deploying such service-specific database solutions. On the other hand, many commentators recognized that S&S is the long term solution. It remains to be seen at this time how fast S&S technology will actually be deployed and whether a mandate will be required by the Commission. However, the Commission should expect pushback from the industry if there are mandates for deploying both short term solutions and a long term solution. Simply stated, mandating implementation of the former will delay implementation of the later.

Deployment of S&S does not preclude a carrier from using the indicated level of attestation to perform call blocking, nor does it require a carrier block calls based on the level of attestation. S&S is predicated on providing information of the call that can be used by the called party or carrier to better decide how they want to handle the call.

II. Comments on Specific Issues

1. Who Can Sign a Call (Par. 30)

The Commission requests feedback in paragraph 30 regarding the ATIS proposal "that, to be designated a service provider allowed to sign calling party information, a provider must have an Operating Company Number (OCN)." Noble Systems believes this approach is too narrow, and that there are many entities without an OCN that should be allowed to sign a call. This includes the entities identified by the Commission, including "certain non-facilities-based VoIP providers, providers of call center services, corporations using multiple outbound service providers, or

software application or device manufacturers" (*Id.)*. The Commission has implicitly accepted this understanding in other portions of the NOI, see, e.g., paragraph 35 and footnote 28, which implicitly and explicitly anticipate authentication occurring by entities other than an exchange carrier handling the call. Restricting this capability to only exchange carriers would concentrate power in an unacceptable manner.

2. Scope of Certificate Coverage (Pars. 30 and 35)

The scope of coverage of a certificate should allow coverage of all calls received by a service provider. Service providers will, in turn, incorporate mechanisms (including contractual mechanisms) for ensuring their subscribers are originating calls using numbers they are assigned or are authorized to use. Violations that are reported to the service provider may result in the service provider taking action based on the terms of service agreed to between the service provider and subscriber.

To the extent flexibility can be provided, it would be desirable for the certificate to be defined to allow different scopes of coverage. Perhaps a first certificate could be allocated to a service provider for general purposes (i.e., all numbers) and a second certificate could be used for specific number ranges, or for some other purpose. In either case, a service provider failing to properly authenticate calls or comply with expected practices could have their certificates revoked. This provides an incentive to ensure proper usage.

The Commission also inquired about enrollment procedures. The described top down approach appears consistent with industry expectations. Further, the third approach identified that facilitates delegation should be allowed. There are various circumstances where a party is authorized to originate calls using another party's calling party number and such calls should be signed as fully attested. This "vouching" between the signing service provider and the other party can occur via contractual arrangements. This delegation approach works when legitimate entities are conducting business. Obviously, illegitimate operators will seek any way to perpetrate their scam, but presuming such illegal calls are reported and the signing service provider is quickly identified, the legitimate parties will quickly work to screen off illegitimate call originators. The

threat of not signing future calls or the revocation of certificates will ensure legitimate operators take action and investigate any "downstream" irregularities.

III. The Need For Defining A Specific Cause Code for Call Blocking

As noted earlier, S&S provides information about a call, which can be used by the called party in determining whether to answer the call or not. The information can also be used by the terminating carrier as criteria for blocking the call. When a call is blocked (whether by the S&S technology or by using a blacklist database), the Commission should mandate that the carrier blocking the call explicitly indicate to the calling party that the call was blocked via an appropriate cause code, as opposed to encountering some other condition (e.g., busy, no answer, etc.).

Today, a call that is blocked often results in a "busy" indication returned to the call originator. This may be reflected in an ISDN/SS7 cause code, an Internet Protocol error code, or via in-band tones. If the call originator believes the call encountered a busy condition, the call originator will likely reattempt the call again. The result is increased call attempts that unnecessarily waste network resources. Further, because the call originator does not know the call was blocked, they have no opportunity to mitigate a potentially incorrect classification of the call. This does not serve the consumer who may not be aware of wanted calls that are being blocked.

The Commission should mandate the use of a unique cause code used in the appropriate signaling system to accurately convey the call was blocked. Without this capability, call originators will not know of potential errors in how their call was processed, and will repeat call origination. This can be decided by the appropriate standards/industry bodies upon the encouragement of the Commission.

Respectfully submitted,

/Karl Koster/
Karl Koster,
Chief IP and Regulatory Counsel
Noble Systems Corporation
1200 Ashwood Parkway
Atlanta, GA 30338
(404) 851-1331 (x1397)