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

In the Matter of	)	CG Docket No. 17-59
	)	
Advanced Methods to Target and Eliminate	)	WC Docket No. 17-97
Unlawful Robocalls	)	
	)	

Reply Comments of Noble Systems Corporation

Directed to the Third Further Notice of Proposed Rulemaking (Call Blocking in a SHAKEN/STIR Framework)

Filed August 23, 2019

Karl Koster
Noble Systems Corporation
1200 Ashwood Parkway
Atlanta, GA 30338

Chief Intellectual Property and
Regulatory Counsel

I. Introduction

Noble Systems Corporation ("Noble Systems") [1] submits these reply comments in response to the initial comments submitted to the Commission's Third Further Notice of Proposed Rulemaking ("FNPRM").[2]

Noble Systems observes that there appears to be consensus (though not unanimity) on certain aspects of carrier-based call blocking services in a SHAKEN/STIR ("S/S") framework. Namely, that carriers providing call blocking should provide appropriate real-time notification when a call is blocked and an opportunity to mitigate or redress an alleged error in blocking. The majority of commentators addressing this subject recognized the need for both the caller and called party (i.e., the consumer) to be informed when a call is blocked and provided an opportunity to redress an alleged error.

Similarly, there was consensus that deployment of S/S will be evolving, and that defining blocking criteria solely on the S/S verification outcome may be premature and undesirable. Caution in performing such blocking was generally admonished. A number of commentators observed that the S/S framework does not provide insight as to the intent of the caller, the contents of the call, nor whether the call can be determined to be wanted/unwanted or legal/illegal.

There are at least two areas on which there was not consensus: a) the need for collecting measurements on the effectiveness of the blocking service, and 2) the critical calls list ("CCL").

II. Topics Which Have Consensus

Though not intended to be a comprehensive summary, there are two notable topics in which consensus appears to have been achieved.

[1] Noble Systems is an international manufacturer of contact center software and a hosted provider of contact center services, with 30+ years' experience in the contact center industry. Noble Systems provides multi-channel processing, voice and data analytics, workforce management, robotics processing automation, and other related services.

[2] Public Notice: Consumer and Governmental Affairs Bureau and Wireline Competition Bureau Announce Comment Dates for Call Blocking and Caller ID Authentication Third Further Notice of Proposed Rulemaking No. 17-59, DA 19-597 (June 26, 2019).

a. Notification and Mitigation of Blocked Calls ("Transparency")

There is consensus related to the need of providing both the caller and the called party (consumer) with transparency as to when a call is blocked.[3] The comments referenced this concept by various terms. Generally the concept of "notification" refers to providing both the caller and the called party with information that a call was blocked. With respect to the called party, this could be accomplished via a portal or a mobile application. With respect to the caller, notification of a call being blocked could be provided in real-time via a signaled error code and an audio intercept. Only one comment was observed advocating against providing the caller with real-time notification that the call was blocked, and the justification was that doing so would inform scammers that their calls were being blocked.[4]

Noble Systems, along with the majority of others that addressed this issue, believe there is a pressing need to inform legitimate callers that their calls are being blocked and this need supersedes any benefit of not informing scammers. The deployment of S/S in the near future is designed to identify spoofed scam calls and its effectiveness should not be masked by providing misleading call treatment to callers. It should also be noted that providing both consumers and callers with "transparency and effective redress options" is included in a pending legislative bill updating the TCPA (the "Stopping Bad Robocalls Act"), which was recently passed by an overwhelming majority of the House of Representatives, thus showing strong bi-partisan support for the need of both transparency and redress for call blocking.[5]

The support for redress (a.k.a. "correction," "a challenge mechanism," or "mitigation") also shows a consensus for allowing callers and consumers to be able to request unblocking. [6] In effect, overriding a specific number from being blocked can be thought of as creating an entry into a consumer's "whitelist" or creating a consumer-defined exception list of calls that should not be blocked.

[3] See e.g., NCTA Comments, p. 14-15; Cloud Computing Alliance Comments, p. 10; Joint Comments of: American Bankers Assoc., ACA International, American Association of Healthcare Administrative Management, American Financial Services Association, Consumer Bankers Association, Credit Union National Association, Edison Electrical Institute, Independent Community Bankers of America, Mortgage Bankers Association, National Association of Federally-Insured Credit Unions, and National Retail Federation, p. 5-6; Sirius XM, p. 6; Comments of Consumer Reports and National Consumer Law Center, p. 10.

[4] First Orion Corp. Comments, p. 11.

[5] H.R. 3375, 116th Congress (2019-2020) Section 8. Text at https://www.congress.gov/bill/116th-congress/house-bill/3375/text.

[6] See e.g., Comments of Consumer Reports and National Consumer Law Center, p. 10.

b. Blocking Based on S/S Verification Outcomes Should be Done with Caution

A number of commentators recognized that not all networks will be able to quickly adopt the S/S framework.[7] Hence, as network deployment of the S/S framework evolves, the number of calls that will be signed will change. Thus, blocking calls based on whether they are signed or based on a particular attestation level, may result in over-blocking initially and lead to unwanted outcomes for the consumer. Thus, it is recognized that blocking services may evolve, and regulations should be flexible to accommodate this evolution.

Noble Systems notes that some commentators indicated that the Commission's prior orders may be obsoleted once S/S is deployed, and advocated for reconsideration of prior orders.[8] The Commission should review the scope of their prior orders, since it presently appears that the Commission has given broad authorization to carriers to block any type of call, provided that the consumer is suitably informed.[9] In the future, once S/S framework is widely deployed, it may be appropriate to modify or limit this authorization.

III. Topics Which Do Not Have Consensus

a. The "Measurement" Issue Remains Disputed

This issue refers to the extent that carriers or analytics providers are obligated to report blocking-related data allowing the Commission to determine or measure the effectiveness of their blocking services.

A fundamental concern with analytics-based blocking is that it is susceptible to 'over-blocking.' Presumably, such problems are avoided if the analytics-based algorithms are "reasonable." However, defining the scope of what is "reasonable" is likely to be a function of whether wanted calls are blocked. Further, a number of commentators requested safeguards to ensure that analytics-based call blocking is not performed in a discriminatory manner.[10]

[7] USTelecom Association Comments, p. 12; NTCA, p. 1-10; WTA, p. 1-5.

[8] TCN Comments, p. 5; ACA International Comments, p. 8.

[9] FCC Declaratory Ruling, Fed. Reg. Vo. 84, No. 121, Monday, June 24, 2019, p. 29387, "The Commission has repeatedly stated that offering call-blocking services does not violate voice service providers' call completion obligations under section 201(b) of the Communications Act of 1934, as amended (the Act), and that consumers have a right to block calls."

[10] See e.g., AARP Comments, p. 13; Alarm Industry Communications Committee Comments, p. 1; INCOMPAS Comments, p. 7; Massachusetts Department of Telecommunications and Cable Comments, p. 7; VON, p. 2.

The determination of whether an algorithm is "reasonable," "effective," "over-inclusive," or "non-discriminatory" can be done in two ways. First, the algorithms can be disclosed and studied to determine whether they would be deficient in any way. This would be complex, as it would require sophisticated expertise to review the algorithms, and would require that analytics companies disclose their algorithms. This approach can be quickly discarded for the obvious reason that analytics companies should not be forced to disclose their proprietary algorithms. The other approach is to simply measure the outcome of the algorithm processing calls, including, for example, the number of calls handled and blocked. Some analytics providers already report this information.[11]

Another proxy for evaluating the "reasonableness" of an algorithm is to review the number of mitigation requests from callers and consumers. A carrier whose consumers never submit an unblocking request would presumably be satisfied with the blocking service as compared to a carrier that receives a high number of unblocking requests. Similarly, callers having issues with their calls being blocked by a particular carrier will be submitting high numbers of mitigation requests to that carrier.

Not surprisingly, some carriers and their analytics providers object to this requirement.[12] In some instances, the reasons are not persuasive. Assuming carriers are required to provide notification of blocking and means to mitigate erroneous blocking, collecting this data is not a new data collection requirement. The number of calls blocked will be known to the analytics provider. As noted by one analytics provider, they already report some of the data they collect.[13] So this requirement would not impose a new data collection requirement, but, rather, merely a new requirement to report existing data. Reporting data that is already collected is not a new data collection requirement and therefore not as burdensome.

This data would provide the Commission with visibility to gauge the relative effectiveness of whether a carrier's algorithms are "reasonable," "discriminatory," "over-inclusive," or otherwise comparatively deficient. Reviewing such data will allow the Commission to identify potential issues in blocking practices and better report on the effectiveness of call blocking.

[11] First Orion Corp. Comments, p. 8, footnote 18.

[12] CTIA Comments, p. 24-25 ("Commission [should] refrain from adopting burdensome reporting and/or public disclosure requirements…"; T-Mobile Comments, p. 12 ("The Commission need not create that mechanism.")

[13] First Orion Corp. Comments, p. 7, footnote 16; p. 10-11.

Adopting a principle of transparency in how blocking is applied is important enough by itself to justify this reporting requirement, which can be accomplished by reporting data that the analytics providers already collect (or will have to collect). It provides necessary visibility into the carriers' practices, which otherwise would be opaque to the Commission.

b. The Critical Call List ("CCL")

A number of commentators advocate creating a critical call list, so much so that it may be appear to reflect a consensus.[14] However, a number of commentators noted that creating the CCL is not so straightforward and have identified concerns.[15] Noble Systems shares these concerns and believes that before deciding whether a CCL is warranted, industry and the Commission should have a complete understanding of the implications and costs of a CCL, and consider whether alternatives are feasible. Any decision should also be based on a clear understanding of how costs will be recovered (i.e., who pays). If those advocating for a CCL are not willing to bear the cost for such an infrastructure, then that mitigates against mandating such a capability. It is all too easy for those not bearing the costs to advocate others to bear the cost of implementing a CCL.

While various aspects related to the CCL were identified in separate comments, a holistic view of all the implications of mandating a CCL should be considered by the Commission and industry. A brief overview is attempted below to identify these aspects.

i. Scope of the Numbers to be Included in a CCL

It is evident that there is divergence as to what types of calls should be in the CCL. Many industry respondents that originate calls take the position (not surprisingly) that their call

[14] See e.g., American Association of Healthcare Administrative Management Comments, p. 2; Comcast Corporation Comments, p. 11; Credit Union National Association Comments, p. 7; T-Mobile USA Comments, p. 2.

[15] Boulder Regional Emergency Telephone Service Authority Comments, p.5 ("Entering these numbers on a Critical Call List could thus make it easier for robocallers to spoof these numbers and make it appear their calls are coming from a trusted authority….″; CTIA Comments, p 21 ("However, developing such a centralized list raises complex issues.); Larimer Emergency Telephone Authority Comments, p. 2("LETA does not believe that the proposed Critical Call List would provide sufficient safeguards or protections to ensure that the most important calls – calls coming in to a PSAP and calls going out from a PSAP – are not erroneously blocked."); RingCentral Inc., p. 9 ("Given the challenges of both a per-provider and centralized Critical Calls List, it is premature to mandate either variety."); U.S. Telecom p. 3 ("…however, USTelecom urges the Commission to proceed with caution before mandating a "Critical Calls List" because it is likely unnecessary with the implementation of SHAKEN/STIR combined with analytics…."); Sprint Corporation Comments, p. 5 ("Sprint believe that the best path forward for critical calls is for the industry to adopt SHAKEN/STIR universally and promptly….").

originations are critical and should be on the CCL.[16] In many cases, consumers would consider a particular call type as critical, but it would be difficult for a third party to objectively make that determination. Some comments indicate that the Commission is the appropriate entity to make the determination of what types of numbers would be eligible.[17] Others advocate for other agencies to have input in reviewing the contents.[18] Likely, this will require the Commission to set up on-going procedures for evaluating such requests, which would also necessitate defining a means of appealing an adverse determination.[19] These requirements are not objectively unreasonable, and illustrate that the issue is more involved than merely agreeing that "important" numbers are to be included in the CCL.

A number of distinct categories of critical calls were collectively identified, and these are listed below, along with potential additional categories.

1. **Local Critical Numbers**. Each municipality will have local fire, police, PSAP, and other local numbers designated as critical.
2. **State Critical Numbers**. Each state will have state-wide emergency centers, first responders, and other state agency numbers designated as critical.
3. **Federal Critical Numbers**. There are a number of federal agencies which will demand that their numbers are designated as critical, such as FEMA, Homeland Security, etc.
4. **Military Critical Numbers**. No doubt various military related numbers would be deemed critical.
5. **National Business Critical Numbers**. Certain business numbers that are national in scope could be considered as critical. These could include, e.g., alarm notifications, fraud notifications, payment delinquency alerts, product safety recalls, etc. Many consumers

[16] American Association of Healthcare Administrative Management Comments, p. 2 (healthcare related calls should qualify for the CCL); Joint Comments of American Bankers Assoc., ACA International, American Association of Healthcare Administrative Management, American Financial Services Association, Consumer Bankers Association, Credit Union National Association, Edison Electrical Institute, Independent Community Bankers of America, Mortgage Bankers Association, National Association of Federally-Insured Credit Unions, and National Retail Federation, p.2; Alarm Industry Communications Committee, p. 1; Consumer Bankers Association, p. 3; Securus Technologies, Inc., p. 6; INCOMPAS, p 12; see also Comments of Consumer Reports and National Consumer Law Center, p. 9, (advocating for various governmental types of numbers included in the CCL).

[17] See e.g., Comcast Corporation Comments, p. 12;

[18] Massachusetts Department of Telecommunications and Cable Comments, p. 7.

[19] TCN Inc. Comments, p. 4; ACA International Comments, p. 13;

receiving such calls may deem types as critical. These calls originate and terminate nationwide and are thus national in scope.

6. **Local Non-Profit, Business Enterprise, and Non-Governmental Organization Critical Numbers**. These are various non-profit and/or business enterprise numbers that are local or regional in scope, which could be considered as critical. These could include, e.g., school notifications, hospitals, doctors' offices, Red Cross, etc.

While there is no current consensus of the exact scope of the CCL, it can be predicted that the scope will only be enlarged over time as more stakeholders seek to have their calls included in the CCL.

c. A Centralized Database Management System May Be Required

The management of these numbers will be complex and it is generally recognized that one approach involves a centralized provider of a database management system ("DBMS").[20]

i. This DBMS will have to offer different types of interfaces to facilitate CCL number registration. For example, a rural police station registering five numbers will not have sophisticated computers to convey their numbers and they would likely have to be served with a phone-based channel, email, or fax to convey or update their telephone numbers. At the other end of the spectrum, a government agency conveying thousands of numbers will require an automated, computerized interface as regular updates would be expected.

ii. The DBMS entity will have to be available 24/7. Due to the nature of the service of facilitating and distributing critical numbers, a fail-safe infrastructure will likely be required.

iii. In addition for standards defining the interfaces for receiving numbers for inclusion on the CCL, standard interface and procedures will have to be defined to distribute the updated critical lists of numbers to the various domestic carriers.

[20] See, e.g., Comcast Corporation Comments, p. 12.

d. Security and Associated Infrastructure Is Required

The database would have to be secure to protect the information.[21] This would likely require the database contents to be encrypted, and this would require a mechanism to allocate, maintain, and track encryption keys among those carriers authorized to receive such information as well as identifying the organizations authorized for providing ongoing input. Presumably, a governance authority would be required to manage the security-related procedures for applying, certifying, and managing the appropriate encryption keys and access to the database.

e. A Vetting Entity is Required

As some have noted, each entity submitting a purportedly critical number to the CCL DBMS must be manually vetted.[22] Each entity would have to be vetted to ensure it is providing numbers for the authorized purpose, and the individual numbers would also have to be vetted. This process must also ensure that bad actors are not attempting to register their numbers as critical so as to circumvent blocking. Anecdotal evidence from analytics providers suggest this has been attempted in conjunction with analytics-based blocking. For example, if alarm notification calls are authorized for inclusion on the CCL, then a company providing notification of an e.g., insurance policy about to lapse should not be allowed to register that number as being an alarm notification call. Further regulatory procedures will be required to define the vetting process. For example, as noted by some commentators, if emergency school notifications are allowed inclusion on the CCL, would this encompass registering numbers from private schools, pre-kindergarten schools, and/or private daycare operators?[23]

f. Compliance/Performance Parameters have to be Monitored

The overall process for placing a number on the CCL must consider: the processing time expected for receiving a request from an entity to register a list of numbers, vetting the entity,

[21] Larimer Emergency Telephone Authority Comments, p. 4 ("Confidentiality and security of the Critical Calls List database is paramount. The list must be protected and secured to prevent an attack. Safeguarding this information is essential.").

[22] Sprint Corporation Comments, p. 5 ("[C]arriers do not have the expertise to vet the thousands of entities around the country seeking to register as critical callers.").

[23] See, e.g., West Telecom Services, LLC Comments, p. 12.

determining whether the numbers are critical, updating the database, and distributing the results. Such activities warrant oversight and compliance. Assuming these tasks are performed by third-party entities (i.e., not a governmental agency), then a likely requirement is that the Commission will have to mandate operational performance requirements and maintain oversight over these third-party entities.

g. Cost Recovery – The Open Question to be Addressed

Establishing and operating a DBMS is of greater complexity than the national do-not-call ("DNC") list database. The DNC database does not require the complex security and vetting that is associated with the CCL database. While the cost is not readily quantified, it would seem comparable in complexity to the NPAC database, which the Commission reported was about $143 million per year to operate.[24] Obviously, providing the vetting service, security management, DBMS services, will each have associated costs. A number of commentators have indicated that end-users should not be required to pay for a blocking service.[25] This does not address the question of how costs will be recovered – i.e., who will pay. In this ecosystem, this leaves few options as to which entities will bear the cost, with carriers the most likely choice.

However, some carriers may opt to avoid blocking calls once S/S is deployed and some commentators note that foregoing call blocking would allow the provider to reduce their costs.[26] It would seem most appropriate, then, to have the carriers that offer analytics based blocking services collectively pay for this infrastructure on a proportional basis. However, this does result in the risk that if certain carriers opt-out from blocking signed calls, then the remaining carriers that are blocking signed calls will bear a larger percentage of the infrastructure cost. This could provide an incentive for carriers to opt-out, and lead to the financial collapse of revenues necessary to support the overall framework for a CCL.

[24] FCC Second Report and Order, CG Docket 17-59, Release Dec. 13, 2018 (FCC18-177), par. 67.

[25] AARP Comments, p. 9; ACA International Comments, p. 13; Massachusetts Department of Telecommunications and Cable Comments, p. 6; but see also Consumer Reports and National Consumer Law Center Comments, p. 10.

[26] Massachusetts Department of Telecommunications and Cable Comments, p. 6.

h. Security – The Overriding Concern

The concept of a "critical call list" is premised on keeping the list secret and secure.[27] Much of the cost and complexity identified is related to keeping the CCL secure. Recall that the list is downloaded to all carriers performing blocking. Further, some comments advocate for a portal where users can access the information.[28] A fundamental question has to be asked, is it realistic to expect that the CCL will be kept secret given the wide dissemination of the contents? Other commentators have voice similar concerns.[29]

Before committing to this path of constructing a CCL and its associated infrastructure, consideration must be given to what happens if the list is disclosed. It is unacceptable to expect that those callers would be required to alter their numbers in the case of a breach. If so, would the entire infrastructure be rendered worthless if security is not maintained? In the case of a breach, would carriers now be forced to block numbers on the CCL if those numbers were suspected to be spoofed? If so, should the CCL DBMS also maintain current information as to whether each number in the CCL is expected to be signed? (In this way, an unsigned or partially attested critical call number could be handled differently from a fully attested critical call number).

Assuming *arguendo* that the CCL is kept secure and never breached, there is the possibility a scammer could easily derive what numbers are on the list. For example, if it is determined that government emergency numbers should be included in the CCL, then a scammer could obtain a list of telephone numbers from a website listing, e.g., FEMA contacts (which are presently published on the Web).

Presumably, S/S will be deployed in the near future, and as such, these critical government numbers should be signed as fully attested. If a scammer spoofs a number on the CCL, then presumably that number would not be signed as fully attested. A question arises why a carrier would then be blocking fully attested calls indicating a critical call number (or any fully attested

[27] Larimer Emergency Telephone Authority Comments, p. 5 ("The Critical Calls List database must be nonpublic and must be protected.")

[28] Larimer Emergency Telephone Authority Comments, p. 4.

[29] T-Mobile USA Comments, p. 10 ("A centralized list of truly critical callers is appealing on its face but presents many complex issues that must be resolved before implementation, including how to maintain its confidentiality and ensure that numbers on the list are not spoofed."); Sprint Corporation, p. 6 ("Any critical calls list will inevitably become public as thousands of carriers and potentially unlimited app developers and analytics entities seek access to it to improve their product's accuracy.").

signed call)?[30] Once calls are fully signed, carriers could manually investigate whether a caller is perpetrating a scam before blocking such calls. This could be done by e.g., calling the number. Does this fundamentally raise a question about the utility of a secret CCL list and the obvious need to keep it secure?

Understanding these answers is necessary to determine whether a CCL is necessary. It is noted that many of the carriers, or their industry associations, are more circumspect on the need for such a list.[31] Many commentators advocating the need for a CCL do not address any of these issues. Other commentators affirm the need for a CCL, but they may be unwilling to commit to bearing the associated costs, noting that end-users should not be paying for such services. Others may affirm the need based for such a CCL, but with an implicit understanding that their calls should be included in the CCL.

Notably, two commentators involved in emergency communications are not so forthcoming to endorse the CCL. "LETA [Larimer Emergency Telephone Authority] does not believe that the proposed Critical Call List would provide sufficient safeguard or protections to ensure that the most important calls – calls coming in to a PSAP and call going out from a PSAP – are not erroneously blocked."[32] In addition, the Boulder Regional Emergency Telephone Service Authority stated that "Entering these numbers on a Critical Call List could thus make it easier for robocallers to spoof these numbers and make it appear their calls are coming from a trusted authority, making called parties more vulnerable to attempts to defraud them."[33] It added: "Inclusion of ENSs [emergency service numbers] on any Critical Call Lists, if accessible by the public or malicious motive, could enable parties to conduct total denial of service…."[34]

i. Other Alternatives

Presumably, in the near future, the majority of critical calls originating in metropolitan areas will have their calls signed and fully attested in a S/S framework.[35] Carriers may modify

[30] See, e.g. Massachusetts Department of Telecommunications and Cable Comments, p. 6 indicating that providers may discontinue call-blocking programs after implementation of SHAKEN/STIR.

[31] See, e.g., USTelecom Comments, p. 9; Sprint Corporation Comments, p. 5.

[32] Larimer Emergency Telephone Authority Comments, p. 2.

[33] Boulder Regional Emergency Telephone Service Authority Comments, p. 5.

[34] *Id*, p. 7.

[35] Furthermore, many of the anticipated critical calls will originate in metropolitan areas are expected to receive initial deployment of S/S sooner as opposed to later. Thus, callers that consider their calls to be critical will demand their

their call blocking algorithms to take into account calls that are signed and fully attested, and allow such calls to normally pass. A carrier may have a lower threshold for blocking unsigned calls compared to blocking signed calls that are fully attested. This raises the question of whether the CCL should only be defined for analytics-based blocking of unsigned calls. If so, then is the CCL necessary in a S/S framework?

While it is true many scams can be originated on signed calls using non-spoofed numbers, likely carriers will be more circumspect in blocking calls having fully attested numbers. Rather than rely on current procedures that may not involve any verification procedures prior to blocking the call, the carrier may opt to process fully attested calls differently, such as:

- manually call back the number and investigate the source of the number and the reason for the calls,
- perform a reverse white-pages lookup of the number to ascertain where it is from (e.g., did it originate from a government agency or one of their customers?),
- refer the matter to regulatory or state authorities for investigation, or
- initiate a "track and trace" and have the originating carrier perform the investigation.

Once calls are signed as fully attested, carriers are likely to be more circumspect before treating the call as "illegal" and blocking it. However, it still remains possible that hackers could compromise a PBX, even one that originates critical calls, causing it to initiate fully authenticated calls.[36] The carrier could, instead, rely on consumers to invoke a track and trace function to identify which calls are presumably illegal.[37] Or, analytics algorithms could label (but not block) such calls to warn consumers of potential scam calls.

carrier upgrade and sign their calls using the S/S framework. For example, a bank sending out nationwide fraud notifications will likely not use a carrier unable to sign their call originations, but will switch to a S/S enabled carrier. Once the caller has their calls signed, many (but not all) such calls will be transmitted end-to-end as a fully attested call.

[36] See, e.g., First Orion Corp. Comments, p. 7, stating that hackers may compromise a PBX of a legitimate organization, causing fully authenticated calls to be initiated. If such numbers were on the CCL list, then this, too, raises questions about whether such calls should be blocked.

[37] The Commission should consider mandating carriers that deploy S/S to also provide consumers with a "call trace" feature, analogous to the service provided today with the "*57" vertical service code. Without this capability, a large benefit of the "track and trace" functionality defined in S/S will be unavailable to consumers, who are the first and most likely source in identifying an illegal call.

The above options do not rely on a national CCL DBMS to distribute critical numbers, nor do they rely on keeping the CCL secure, nor do they require any vetting of the numbers. Further, the above alternatives can be tested and evaluated with minimal regulation, cost, and in a rapid timeframe. Doing so leaves open the option for defining a CCL list in the future, if the Commission deems necessary.

IV. Conclusion

Blocking calls based on analytics is currently an imperfect service. Because of that, it is appropriate to mandate certain related services that must be offered by each carrier providing a carrier-based blocking service. The consumer and caller should be provided with transparency as to which of their calls are being blocked. In addition, means must be provided for consumers and callers to mitigate potential errors. In the case of analytics-based blocking, the Commission should further require that carriers report data that they collect to allow the Commission to gauge the efficiency and effectiveness of call blocking algorithms. No new data collection requirements are foreseen, but a new data reporting requirement is needed.

The Commission should proceed cautiously with respect to defining further call blocking regulations as networks will evolve in their deployment of the S/S framework. Likely, further information and experience on deploying S/S will be forthcoming impacting how such regulations should be defined.

On the issue of creating a CCL, the Commission should further investigate how this infrastructure would work, how it would be paid for, who would pay, and define a contingency plan addressing the possibility if the CCL is breached or its contents are surmised based on existing public information. It very well may be that carriers evolve their analytics algorithms after S/S is deployed to the point that a CCL is no longer needed.

Respectfully submitted on August 23, 2019,

/Karl Koster/

Karl Koster
Chief Intellectual Property and Regulatory Counsel,
Noble Systems Corporation
1200 Ashwood Parkway
Suite 300
Atlanta, GA 30338
(404) 851-1331
kkoster@noblesystems.com