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

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

Comments of Noble Systems Corporation

Filed August 31, 2020

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

Chief Intellectual Property and Regulatory Counsel

Table of Contents

EXECUTIVE SUMMARY

Noble Systems Corporation ("Noble Systems")[1] submits these comments in response to the Consumer and Governmental Affairs Bureau's ("Bureau") request for comments directed to the Commission's Third Report and Order, Order on Reconsideration, and Fourth Further Notice of Proposed Rulemaking ("*Third Report and Order"* and "*NPRM"* respectively), adopted by the Commission on July 16. 2020.[2] Noble Systems supports the Commission's goal of reducing robocalls and restore consumer trust in the national telephony infrastructure.

A variety of tools are required to achieve this goal and call blocking is an important tool in reducing illegal calls. It is expected that service providers will further modify their analytics algorithms to use call authentication information to better target illegal and unwanted calls. However, it is expected and even accepted to a certain level that mistakes will be made. To accommodate this possibility, it is necessary to inform callers when their calls are being blocked and to provide rapid redress. Without either function, callers are not provided with the Congressionally mandated transparency and redress capabilities. Specifically, the TRACED Act requires the Commission to develop rules to ensure transparency is provided to the both the called party and the caller with respect to call blocking. The approach to fulfill this mandate of ensuring transparency is clear - the Commission should develop regulations requiring a per-call blocking notification ("PCBN") for callers. Doing so allows the Commission to not only meet its obligations of providing transparency, but also meet its other obligations under the TRACED Act.

The Commission should clarify its regulations with respect to providing safe harbor to voice service providers when they inadvertently block calls and how callers are provided redress when calls are erroneously blocked. As currently defined, the regulations are unclear with respect to the obligations of service providers as to how they are to provide redress.

---

[1] Noble Systems is a manufacturer of contact center software and an international hosted provider of contact center related 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] Consumer and Governmental Affairs Bureau Seeks Input for Report on Call Blocking, In the Matters of Advanced Methods to Target and Eliminate Unlawful Robocalls and Call Authentication Trust Anchor, CG Docket No. 17-59, WC Docket No. 17-97, DA 19-1312 (released December 20, 2019).

In addition, the Commission should consider empowering consumers with the ability to identify on a per-call basis, which calls they receive are unwanted or illegal by defining a customer originated trace request. This is intended to serve as a basis to allow consumers to identify illegal calls.

Finally, the Commission should avoid addressing issues of call labeling at this time. There does not appear to be a path for success in regulating this area in the immediate future. Furthermore, the offering of new services, such as enhanced calling name, may reduce the utility of call labeling. This may render moot the need for regulations pertaining to call labelling.

I. INTRODUCTION

These comments largely focus on two issues. First, the need is discussed for providing a per-call blocking notification ("PCBN"), which is mandated as part of the TRACED Act's mandate of ensuring "transparency" is provided to callers when their calls are blocked. Providing this notification also allows the Commission to meet its other mandates in the TRACED Act.

Second, the issue of safe harbor for inadvertent blocking is discussed. The concept of a safe-harbor implies a quid-pro-quo. That is, a service provider meeting a defined obligation receives a safe harbor in return when inadvertently blocking a call. The obligation is (or should be) related in part to the concept of providing "redress." The TRACED Act evidences that Congress recognized that service providers can make mistakes by inadvertently blocking calls. Further, Congress provided a safe harbor to avoid penalizing service providers when they make this type of mistake. But, Congress also mandated service providers implement a redress mechanism to fix such mistakes.

The Commission seeks comments on their safe harbor regulations, and it is unclear what obligation exists on service providers to fix their blocking mistakes after they are made aware of them. The question arises whether a mistake of inadvertently blocking a call encompasses subsequently blocking calls from that calling number after being informed via the redress mechanism that the call should not have been blocked. Furthermore, it is unclear under what circumstances a voice service provider could lose their safe harbor. A framework is proposed wherein clearly defined obligations are set forth clarifying under what conditions a safe harbor is granted, when calls can be blocked under the auspices of the safe harbor, and how service providers should address redress requests to avoid losing their safe harbor.

II. PER-CALL BLOCKING NOTIFICATION ("PCBN")

The Commission seeks input regarding its transparency regulations found in the *Third Report and Order*. Specifically:

> We seek comment on providing transparency and effective redress options for both consumers and callers. Are the steps we take in the *Third Report and Order* sufficient? What further steps might we take to ensure that both consumers and callers are provided with transparency and effective redress options?[3]

For the various reasons indicated below, the Commission should mandate service providers blocking calls provide a uniform PCBN to callers.

A. The Commission Has A Statutory Mandate to Define a PCBN

In the *Third Report and Order,* the Commission declined at that time to require service providers provide a PCBN when a call is blocked. But the TRACED Act requires the Commission to take actions to ensure this is done:

> [n]ot later than 1 year after the date of the enactment of this subsection, the Commission shall take a final agency action to ensure the robocall blocking services provided…(A) are provided with transparency and effective redress options for both (i) consumers; and (ii) callers…."[4]

The common understanding among industry is that providing "transparency … for… callers" with respect to robocall blocking services involves providing a PCBN, i.e., notification of some form to the caller that the call is blocked. This could be provided via an intercept announcement[5] and/or a SIP based error code. This feature has been repeatedly identified to the Commission as a critical feature required by callers to know when their call has been blocked, including by Noble Systems since at least since 2017.[6] It is possible that this requirement of transparency could be provided to the caller in other ways, including some rather fanciful and complicated mechanisms, such as allowing the caller to launch real-time queries to a database operated by the terminating service provider that responds with information about whether a particular call was blocked. However, such ways are impractical and nor has there been any serious proposals for defining such fanciful and complicated architectures. Consequently, there are

[3] *Fourth Further Notice of Proposed Rulemaking,* CG Docket No. 17-59, adopted July 16, 2020 ("NPRM"), par. 92 (footnotes omitted).
[4] TRACED Act, Section 10(b)(1).
[5] These announcements would "intercept" the normal routing of a call by redirecting the call to an announcement system that plays an announcement reporting an abnormal condition. For example, a caller dialing an unassigned telephone number will hear an announcement that the number is not in service and to check their directory.
[6] See, e.g., Noble Systems Comments, CG 17-59, July 3, 2017, at 10.

no other approaches presented to the Commission or proposed by the industry for meeting the statutory 'transparency' mandate with respect to callers. Thus, providing "transparency…for…callers" is practically understood to be a mechanism in which the caller is provided a PCBN via an intercept announcement and/or a SIP error code. Consequently, meeting the statutory mandate of providing transparency to callers involves providing the PCBN to the caller, not some other type of protection or capability.

The Commission has stated: "We decline at this time to require other protections we sought comment on in the *Call Blocking Declaratory Ruling and Further Notice*, such as requiring voice service providers to send SIP or Integrated Services Digital Network User Part (ISUP) codes when calls are blocked."[7] It can only be assumed that the Commission has not yet adopted such regulations at this time and expects to do so by end of this year. Failure to adopt a final agency action by the end of this year could be interpreted as the Commission abdicating this statutory mandate in the TRACED Act.

The Commission continues by stating:

> Though many commenters, particularly those placing calls, supported extensive protections, others argued that these protections are unnecessary and potentially harmful. We agree with commenters that support allowing voice service providers flexibility for now and pending further developments in the record.[8]

If this is the final Commission's disposition in the *Third Report and Order* regarding providing transparency to the caller, then this would not meet the statute's mandate "to ***ensure*** the robocall blocking services … are provided with transparency… for callers…." Ensuring transparency for callers requires each service provider provide an *unambiguous* notification to the caller that a call was blocked. Presumably, with the comments received by the Commission via this NPRM, the record will have been sufficiently developed to support the Commission defining regulations on providing a PCBN.

Some carriers have been using mechanisms, such as providing a 'busy' indication to blocked calls, but this does not provide transparency to the caller. This approach is not accurate because the called party is not actually busy and thus the busy indication is an inaccurate response

[7] *Third Report and Order*, par. 59.
[88] *Third Report and Order*, par. 59, citations omitted.

provided in lieu of more accurate information. As a result, providing a busy indication (or some other existing indication reflecting some other event) masks the actual event of call blocking. This does not ensure 'transparency' is provided to the caller. Rather, this is the exact opposite of transparency; it is an opaque indication. Providing a misleading busy indication deliberately confuses the caller as to whether the call was blocked or actually encountered busy. Many callers encountering a busy would reattempt the call again, which wastes further time and resources. This is an inherent problem that also occurs when repurposing, for example, an existing SIP error code or call termination treatment that indicates some other condition. No doubt voice service providers were hesitant to create a new, non-standard indication for a newly authorized blocking capability and had to provide some form of call termination treatment. Hence, they selected an existing call termination treatment to provide to the caller. But, creating ambiguity to the caller should not be equated with providing transparency.

The Commission has been fully aware since: 1) prior to the introduction of the TRACED Act, 2) during the time the TRACED Act was being introduced and considered by Congress, and 3) since the passage of the TRACED Act on December 30, 2019, that callers have been asking for transparency when calls are blocked by requiring service providers send a per-call blocking notification. The record does not support any reason why the Commission should not fulfill its mandate by December 30, 2020.

The regulations that are to be defined by the Commission by year's end do not necessarily have to require voice service providers implement the mechanism by year's end. The Commission can define a transition period to accommodate network migration by voice service providers. However, it is vital to have a goal of providing a consistent form of notification that callers can rely upon to unambiguously indicate a call was blocked. Failure to do so can only be interpreted as not meeting the statutory requirement of ensuring transparency for callers.

B. The PCBN Is Required For The Commission to Meet Its Other Mandates

There are various other mandates in the TRACED Act that are facilitated by the Commission mandating a PCBN. To understand the role of the PCBN in meeting these mandates, it should be recognized that there has been a fundamental and recurring problem in the robocall blocking ecosystem that has not been resolved. Specifically, voice service providers are unable to

accurately ascertain whether a particular call is, in fact, illegal or unwanted by the called party. Service providers have applied analytics in an attempt to accurately ascertain this, but errors occur. Experience has shown that analytics providers claim a very low error rate while call originators in certain industries, such as debt collectors, allege a high error rate of over-blocking of their calls. Various studies have been conducted and reported to the Commission, but frequently these are based on assumptions or using data that is limited in scope. The lack of unambiguous data has hampered analysis of the overall scope of call blocking.

Providing a PCBN to a caller allows the caller to unambiguously collect and analyze data as to how their calls are treated. Without a PCBN, the caller is unable to accurately track what calls are blocked. For example, without a PCBN, a call originator can at best allege that "some unknown quantity of calls originating from this calling party telephone number are suspected of being blocked during an estimated time period." That is not actionable data. Neither the caller, voice service provider, analytics provider, nor the Commission can use a nebulous allegation of some calls being blocked as a basis to act or evaluate the scope of an issue.

However, if a PCBN notification is received by a caller, its occurrence and frequency can be tracked and analyzed. The caller can analyze, for example, which percentage of calls using a specific calling party number are blocked by service provider X versus service provider Y. A caller having such data could support a specific allegation of, e.g., "12% of calls made using calling party number (404) 555-1212 between June 1 and July 1 were blocked by service provider X, but 1% were blocked by service provider Y." That is actionable data.

Importantly, this does not impose a data collection requirement on the service provider, but on the caller. Callers wishing to confirm exactly what has happen with their calls can invest in the appropriate infrastructure for such data collection and analysis. Conveniently, many contact center operators already collect and track data pertaining to their call originations and their call outcomes. Call outcomes of busy, no answer, answered, etc. are already being recorded and tracked. This would only necessitate adding another call outcome category, i.e., "blocked." Consequently, tracking the call disposition as having been blocked is not a significant infrastructure upgrade for many callers. With the PCBN, the caller can now precisely track when blocking occurs. Now, callers would have data to support an allegation of unreasonable blocking. Thus, the PCBN

provides actionable, concrete data to callers. And, as discussed below, there are other compelling reasons to mandate the PCBN.

a) The PCBN Is Useful for Ascertaining When a Calling Party Needs to Verify Their Call Authentication Information

The TRACED Act requires the Commission "to permit a calling party adversely affected by the information provided by the call authentication frameworks…to verify the authenticity of the calling party's calls."[9]

In the near future, a calling party will likely know if/when their originating service provider is authenticating its calls. The calling party will expect/know that their calls using the appropriate calling party number will receive full "A" level authentication. Likely, the originating service provider will inform the calling party when their calls will be fully authenticated, which may be communicated to the caller by an account manager of the service provider. The calling party will expect that these calls will not be blocked because of incorrect authentication or faulty authentication.

If the call is not blocked, then there is likely not much concern by the calling party as to their verification status of their call authentication. A call that is not blocked is likely to not contain call authentication errors. The caller may presume, with some probability, that there are no immediate problems.

However, once a caller learns that its calls are being blocked, the situation is different. Urgent identification and resolution is needed by the calling party. If a call is blocked, then it may be due faulty call authentication information (or other problems). Certainly, if the call authentication information is defective in some way, it is more than likely that the call will be blocked by a terminating service provider. Providing a PCBN provides a clear signal to the caller that something is amiss. In such a situation, the particular cause for blocking could be further narrowed by including an appropriately defined SIP error code to distinguish between call blocking based on a call authentication error or blocking by the application of analytics. At a minimum, the

[9] TRACED Act, Section 4 (c)(1)(C).

PCBN provides immediate information to the calling party that some condition has adversely impacted them and appropriate investigation should indicate the cause.

While it is possible to develop any number of complicated automated schemes to allow the calling party to automatically verify the authenticity of their calls, implementing systems for automatically providing this information in real-time to a caller in response to a query would be burdensome for most voice service providers. Fundamentally, the calling party primarily needs to know if/when there is a problem. The secondary issue after a problem is reported is to learn what is the cause of the problem. The PCBN provides an indication of a problem in real-time and partially addresses the caller's needs. The inclusion of a newly defined SIP error code in the PCBN could be sufficient to indicate the particular reason why the call did not complete. If the error code is not conclusive, then at that point, the calling party could seek manual investigation (i.e., calling their originating service provider's technical customer support) to verify the authenticity of the calling party's calls.

On the other hand, without a PCBN, the calling party is likely to frequently enquire to the originating service provider about the status the authenticity of the calling party's calls whenever a problem of any form is suspected. This is likely to cause the originating service provider to respond to more requests than needed. Consequently, providing a PCBN facilitates this requirement of the TRACE Act and reduces the burden on the originating service provider to field duplicative inquiries from callers. Thus, providing a PCBN can address to some extent the need of a caller to verify their call's authentication status.

b) The PCBN is Effective to Facilitate a Consumer to Determine Whether Wanted Calls Are Being Blocked

The Commission states that "consumers can achieve redress either through opting out or by working with their terminating voice service provider to ensure that wanted calls are not blocked in the future. Absent a list of blocked calls, however, a consumer may not know that they

are missing calls they would prefer to receive."[10] The Commission then asks, "Are there other means through which we could provide transparency and effective redress to consumers?"[11]

While providing a list of blocked calls to the consumer is useful to allow them to ascertain or confirm whether they missed any wanted calls, this by itself, it is woefully deficient. Many times, the consumer does not even know that a wanted call was missed until after it is too late to mitigate the situation. However, in many instances, the *caller* knows that the consumer wants to receive the call and knows that they missed a wanted call.

Consider the following example. A bank contacts its customer about a potentially fraudulent charge on their credit card, but the call is blocked. It is a time sensitive matter and failure to contact the consumer may result in cancelling the consumer's credit card. The customer, however, is not immediately aware of that blocked call. Are we expecting the customer will check their blocked call list each day on their smartphone on the chance that a bank credit card fraud notification call was blocked? Are we expecting that if the customer is notified of a blocked call that the customer will recognize the number of the bank and ascertain it was a wanted call, i.e., a potential fraud notification call? Would we expect the consumer to call back each blocked call on the blocked call list to ascertain why the call was made to ascertain whether it was wanted? The answers are obvious: consumers will rarely periodically check their blocked call list, they will not recognize the number of the caller in most cases, and they will not know whether the call was, in fact, wanted. In the above example, the consumer would not know of the blocked call and their credit card could be cancelled. Likely, only after discovering their credit card was cancelled would the consumer call their bank and then be informed that a call was attempted, but they could not be reached. Then, the consumer may access their blocked call list to verify whether this was true. The harm is not mitigated by providing the called party with a blocked call list that they can check. While this does not negate the need for providing a blocked call list, the Commission should not believe it avoids the consumer from missing a wanted call and fully addresses the consumer's needs.

However, if the caller (i.e., the bank originating the call) knew that the call was blocked because it received a PCBN, then the bank could temporarily suspend cancelation of the card and

[10] NPRM, par. 111.
[11] Id.

use an alternative method of communication to reach the consumer, e.g., sending a text to the consumer's wireless number, sending an email, or originating the call using another calling party number that is not being blocked. This is only possible if the bank is informed the call was blocked.

No doubt, if the consumer is asked whether a PBCN should be provided to their bank in this situation, they would confirm it should be provided. Does anyone seriously propose that consumers should be expected to proactively inquire which telephone numbers are used by each business they deal with and then proactively manually enter their numbers on a do-not-block list? Mandating voice service providers provide a PCBN is actually *a pro-consumer benefit* of providing *consumers* with transparency with respect to which calls are being blocked. Thus, mandating voice service providers send a PCBN to the caller aids the Commission in meeting its mandate of providing consumers with transparency.

The above hypothetical example can be applied to the context of the alarm industry. The Commission addressed a petition on reconsideration by the alarm industry, stating:

> We recognize that alarm company notifications can be extremely important, particularly when it is a question of whether to dispatch emergency services. We encourage alarm companies to take advantage of our requirement in this *Order* that terminating voice service providers that block calls provide a single point of contact for call-blocking issues, and to educate their customers that alarm calls may be blocked if the customer chooses not to opt out of their voice service provider's blocking program.[12]

The alarm industry would similarly want to know when a call they originate is blocked. It is fair to assume their customers want to receive such calls. No one would expect such customers to peruse their blocked call lists to know when a wanted call was blocked. Without a PCBN, the system is designed to fail the customer (at least in some instances). This does not restore trust in the telephone network when it is needed the most. No doubt there are other many business examples of where a given call would be considered critical by the called party.

c) The PCBN is Effective to Ensure There is No Discrimination in Blocking

[12] *Third Report and Order*, par. 75.

The Commission has stated in the *Third Report and Oder* that "we reiterate that voice service providers must apply analytics reasonably in a nondiscriminatory, competitively neutral manner."[13] There is the possibility that calls from one caller could be blocked in an uncompetitive manner. By providing a PCBN, a caller would have data as to exactly which of their calls were blocked. The blocking rates could be compared among and between different callers. A caller would know for example: "X% of 500 calls originating using calling party number 404-555-1212 were blocked by Carrier A, but only Y% of 500 calls using the same calling party number were blocked by Carrier B." This is concrete and actionable date. The Commission could analyze such data, if required, to ensure that its mandate is being applied. Callers would have concrete data to confirm or rebut whether their calls were over-blocked or encountered anti-competitive treatment.

The Commission must have a framework to evaluate whether its mandates are being followed. Data is the basis upon which to make those evaluations. Without a PCBN, the Commission could only evaluate whether a service provider is applying analytics in a discriminatory manner by requiring the service provider to keep and produce records of each call being blocked. This is a non-trivial data collection and retention requirement on voice service providers. The alternative is for voice service providers to send a PCBN that allows callers to ascertain whether service providers are acting in a discriminatory manner in blocking calls. Thus, requiring service providers to implement a PCBN facilitates the Commission meeting its mandate of ensuring analytics are applied in a nondiscriminatory manner.

d) The PCBN is Effective to Ensure Emergency Calls are Not Blocked

The TRACE Act requires the Commission to develop regulations to ensure service providers are making "all reasonable efforts to avoid blocking emergency public safety calls." [14] The Commission has stated it is a priority to ensure such calls are not blocked.[15]

An effective manner of measuring whether this occurs is to require service providers implement a PCBN for all calls. If a public safety call (i.e., an "emergency call") is being made and erroneously blocked, the caller will know when each call is blocked, provided a PCBN is

[13] NPRM, par. 32.
[14] *Third Report and Order*, par. 67.
[15] Id.

received. The PCBN provides concrete data to the caller as to when and how often their emergency calls are being blocked. Without a PCBN, the emergency caller is left making the same nebulous allegation previously identified, namely e.g., "some emergency calls are suspected of having been blocked at some time, but no particular instance can be identified." Contrast that with being able to track each instance and its time. Then, the emergency caller could allege with specificity that e.g., "1.3% of calls were blocked between June 1 and July 1, and here is list of when each call was blocked."

Without actionable data, measuring the scope of this important issue is hampered. Over the last several years, it is evident how the lack of concrete data has resulted in conflicting anecdotal evidence. Analytics companies claim that erroneously blocked calls are extremely rare, while some callers claim it is frequent. The scope of this problem cannot be measured without collecting data provided by the PCBN. It is unclear how the Commission can meet this mandate without requiring a PCBN. Requiring a PCBN facilitates the Commission meeting its mandate of ensuring that emergency calls are not being blocked.

e) The PCBN Has a Role in Verifying Whether Reasonable Analytics Are Being Used

The measurement of the reasonableness of an analytics algorithm is ultimately determined on its outcome, i.e., which calls are being blocked. The algorithms themselves are complicated and proprietary. It is not reasonable to expect the Commission would ever evaluate the programming code implementing an algorithm to determine whether the expected outcome is reasonable or not. Rather, the actual outcome of the analytics would be measured – i.e., what calls were blocked, versus not blocked. Further, reviewing which calls are blocked by an algorithm does not require disclosure of the details of the algorithm itself.

For example, assuming a caller receives a PCBN, the caller would know if e.g., certain calls from a telephone number were blocked at a specific time. The caller would know, e.g., when prior calls originated using that telephone number were not blocked. The caller could develop facts using actionable data that could raise issues as to whether the analytics' outcomes were reasonable or not.

If there is no PCBN mandate, then the caller cannot offer such evidence. Rather, it would be necessary to rely on data maintained by the service providers. This would require that service providers implement a new data collection requirement and maintain information as to which calls were blocked and when. Of course, without a PCBN provided to the caller, callers can only make nebulous allegations that the analytics applied are unreasonable. So, the Commission should expect to address a large number of speculative allegations than otherwise would occur. This approach does not help the Commission meet its goals. Thus, if the Commission requires service providers implement a PCBN, the Commission can potentially receive data from callers that can be easily reviewed to ensure that reasonable analytics are employed.

f) Failing to Mandate a PCBN Effectively Renders the Redress Mechanism Moot

The function of providing a PCBN to the caller goes hand-in-hand with providing a redress mechanism for caller. As noted by the Cloud Communications Alliance in their prior comments:

> Notification of blocking is critical. Callers need to know that the calls are being rejected due to blocking and by whom so that they can promptly invoke the blocking entity's mechanism to reverse blocking of legitimate calls.[16]

It does not make sense to require a redress mechanism, but not inform the caller when their call is blocked. Stated another way, the Commission is proposing to require service providers to accept and timely process requests from callers to mitigate an erroneously blocked call, but the Commission had not presently required service providers to inform callers when their call is blocked. This logic of mandating one, but not the other, does not appear defensible.

Similarly, it seems non-sensical to conclude that Congress mandated the redress mechanism, but then did not intend callers to be informed when their call is blocked. Rather, the language in the TRACE Act explicitly requires "transparency with effective redress options" for callers and this can only be interpreted that Congress intended for callers to know when their calls are blocked so they could seek redress in an effective manner. Providing a channel to callers to identify erroneously blocked calls, but not informing callers when this occurs, is not providing an *effective* redress option to callers.

[16] CCA Comments, July 24, 2019, at 10.

Further, it is difficult to envision how effective redress can provided by the service provider if the caller cannot identify with specificity which calls were allegedly blocked. The analytics provider cannot be expected to determine whether a problem exists, let alone how to solve it, if the caller is able to generally allege: "some of my calls may have been blocked by you in the past." Without knowing what particular calls and at what times, the service provider cannot provide effective redress. A few commentators have indicted the PCBN should not be provided to callers, but they have indicated how service providers could provide effective redress in response to such a general allegation from a caller.

In project planning parlance, this type of system design is known as a "setup for failure" because effective redress cannot occur.[17] In this case, it is the callers who bear the adverse consequences.

Consequently, it is unclear how the Commission could define regulations ensuring callers have effective redress when service providers cannot know the scope of the problem to correct. If the caller is not provided with a PCBN by the service provider, then the caller cannot clearly identify which calls were allegedly erroneously blocked. The Commission cannot meet its obligation of defining regulations mandating effective redress if it does not mandate service providers implement a PCBN.

C. The Reasoning Suggested for Not Mandating the PCBN, if Adopted, is Arbitrary and Capricious

The Commission addresses its decision to not require a PCBN by stating: "Though many commenters, particularly those placing calls, supported extensive protections, other argued that these protections are unnecessary and potentially harmful."[18] Citation is given to comments from CTIA, T-Mobile, and TNS. Neither the July 24, 2019 comments of T-Mobile (i.e., either page 9 therein or otherwise) nor the July 24, 2019 comments of TNS explicitly address the necessity or harmfulness of PCBN. Thus, it is not clear how those comments create a record supporting the Commission's assertion.

[17] "'Setting up to fail' is a phrase denoting a no-win situation designed in such a way that the person in the situation cannot succeed at the task which they have been assigned." (Wikipedia, "Setting up to fail.")
[18] *Third Report and Order*, par. 59.

The comments of CTIA actually do explicitly address the PCBN. They state:

> For example, several commenters urge the Commission to require providers to use standardized notification procedures, such as SIP code intercept messages, to inform callers when their calls have been blocked. As a general matter, requiring all providers to use uniform solutions will actually tip off bad actors that their methods are not working, and encourage them to mount new points of attack to circumvent call blocking tools. What's more, forcing providers to alter or rebuild their solutions will drain resources and increase the burden on those trying in earnest to fight illegal robocallers. The Commission should allow providers to offer a variety of solutions, and continue to innovate and adapt their tools as the problem demands.[19]

The argument is essentially that a uniform PCBN is harmful because it will "tip off" bad actors. This comment was echoed by First Orion, as well. "[S]uch a notification would serve primarily to alert illegal callers that they should switch tactics in order to evade detection."[20]

It is not clear whether the Commission merely identifies these as comments advocating against providing a PCBN or agrees with them as a basis for not mandating a PCBN. If adopted as a basis for not mandating a PCBN, then these reasons are deficient and positions the Commission as adopting a capricious and arbitrary basis for not requiring the PCBN.

a) The Allegation PCBN Is Harmful Is Not Supported by Evidence

Aside from the allegation that such a notification would serve primarily to alert illegal callers to switch tactics, no empirical evidence is offered in the record support this allegation. Rather, at best conclusory statements are offered.

Further, this ignores the significant benefit offered to callers who would know which calls are blocked, so the allegation it "would serve primarily" to tip off bad actors does not perform any comparative analysis of the benefits provided compared to the alleged harm of providing a PCBN. It ignores that the notification would serve to primarily inform callers when a call was blocked so legitimate callers could seek redress.

---

[19] CTIA Reply Comments, Aug. 23, 2019, at 7 (citations omitted).

[20] First Orion Comments, July 24, 2019, at 11.

It is flawed logic to assume a PCBN should not be provided to "tip off" bad actors because they would do something else. First, such bad actors may actually stop originating fraudulent calls! That is a good outcome. If the intent is that scammers should not be informed so they can continue their illegal calls and so that voice service providers can continue blocking them, then that appears to be perverse logic.

The proliferation of robocall scams is because there can be a significant return on minimal efforts. The return is arguably profitable as millions of dollars are scammed each year. The effort is low and is fueled by the low cost in originating calls, universal access/internetworking via the Internet, and the ease in which calling party numbers could be spoofed in SIP. A PCBN explicitly informs the scammer their efforts are not going to be fruitful and they might as well cease originating calls immediately. Providing a scammer with a PCBN would likely cause them to cease scam calls. Granted, scammers may instead pursue some other illegal activity or other form illegal calls, but this is always a possibility. If that logic is taken to the extreme, then any protective measures to discourage fraud should be eliminated. No one is willing to extend that logic in other situations.

Another reason the logic is flawed is that callers originating illegal calls that are blocked *already know* at a general level that their calls are being blocked. Callers know when their call answering rates drop off or when there is an increase in their calls being routed to an intercept or voicemail box. Evidence of this is borne out in contact centers that presently monitor call outcomes and replace the calling party number based on the calls being erroneously over-blocked. That illegal scammers also know this is evidenced by the rise of neighbor spoofing (where the calling party number is changed on a per-call basis in an attempt to avoid blocking algorithms.) Unfortunately, it is incorrect to presume that contact center operators originating illegal calls somehow don't understand this aspect.

Thus, while a legitimate contact center operator may know generally that their calls are being blocked, they do not know with certainty whether a specific call has been blocked. Thus, this general knowledge does not negate the need for callers to know on a per-call basis when a specific call is blocked.

It takes little analysis to realize that the argument that scammers would be 'tipped-off' is not persuasive. However, the more plausible argument is not very persuasive, namely that "forcing

providers to alter or rebuild their solutions will drain resources and increase the burden on those trying in earnest to fight illegal robocallers."[21] In other words, certain service providers don't want to be bothered, nor expend resources, to provide the statutory required transparency to callers. That is not a persuasive argument for the Commission to accept and does not justify why the statutory mandate should be ignored.

Applying this same logic of not wanting to 'tip-off' bad actors originating illegal calls results in a perverse and inconsistent framework in other areas. For example, the Commission has defined procedures allowing "Bad-Actor Service Providers" to be blocked, but requires notifying them first that they are carrying bad traffic and waiting at least 48 hours to allow them to take effective mitigation measures before calls may be blocked.[22] This provides an explicit notification that calls will be blocked, and by the same logic, "tips off" bad-actor service providers, thereby allowing them to switch tactics. By applying the same poor logic, such notification should not occur and their calls should be blocked without informing the bad-actors.[23]

Applying this same logic to the STIR/SHAKEN architecture would also result in a unworkable framework. This same logic would suggest eliminating all the potential (and useful) error diagnostic codes defined to report potential errors. For example, an originating carrier may be informed via various signaling mechanisms that a certificate used on a call is in error.[24] Such useful information is helpful in diagnosing problems. But, such errors can also occur because of nefarious and deliberate usage of incorrect or counterfeit certificates by potential bad-actor service providers. Should all such diagnostic error codes be similarly stripped from the STIR/SHAKEN architecture because sending these might 'tip off' a bad-actor service provider in certain cases? No one is proposing applying that same logic in this framework because it simply does not make sense.

Finally, evidence that this logic is faulty is borne out by the Commission's report that various service providers *are, in fact, currently providing different forms of per-call notification*. The Commission released its report (ironically on the same day the draft Report and Order was

[21] CTIA Reply Comments, Aug. 23, 2019, at 7.
[22] Par. 37 and 38.
[23] Or, perhaps their calls should not be blocked at all, because the call originators might then switch tactics and try some other way to originate scam calls?
[24] See, e.g., ATIS-1000074E-SIP Forum TWG-10-E, Section 5.3.2 "Verification Error Conditions", pages 12-13.

made available) entitled "Call Blocking Tools Now Substantially Available to Consumers: Report on Call Blocking (June 2020). That report details how various service providers are providing various forms of PCBN:

- AT&T: "When a blocked line calls a Mobility, U-verse, Prepaid, or Cricket customer, the calling party will hear an intercept announcement, which includes a toll-free number to call if they believe they were blocked in error." (P. 12.)
- Cox Communications: "Both of these features provide calling parties an intercept message when their calls are blocked." (P. 15-16.)
- Verizon: "Verizon sends Release Code 603 ('denied') for all calls blocked in the network." (P. 17.)
- Vonage: "Anonymous Call Block informs calls with blocked caller ID that the call cannot be completed until they unblock the caller ID." (P. 19.)
- Nomorobo: "For VoIP landline customer, blocked callers receive a call intercept message." (P. 22-23.)

If the Commission believes that such blocking notifications are, in fact, truly harmful, then the Commission should either take immediate action to prevent these service providers from causing further harm. The alternative, which is preferable, is that the Commission should reject the logic that providing a PCBN would be harmful.

Scammers will cease originating calls upon learning they are blocked. That is a good outcome, not a harmful one. To argue that service providers should not notify the caller that their calls are being blocked so that the caller would presumably continue originating calls that are being blocked is a perverse application of logic. Scammers will find a way to take advantage of any systemic weaknesses regardless of whether a PCBN is provided or not. But failing to provide a PCBN causes significant harm to legitimate callers when they do not know their call is being blocked. Thus, the argument that a PCBN should not be provided because it is harmful should be discarded once and for all.

b) The Allegation the PCBM is Not Necessary Is Inconsistent with the TRACED Act

The TRACED Act states that the Commission should take final agency action to ensure blocking services are "(A) are provided with transparency and effective redress options for both (i) consumers; and (ii) callers…." [25] The fact that the TRACED Act mandates development of regulations to ensure that transparency is provided to callers clearly demonstrates that it is incorrect to conclude that the PCBN is not necessary. There no other mechanism defined that provides transparency to callers with respect to call blocking and thus there is no compelling argument that this capability is not needed. The argument that the PCBN is not needed directly contracts the mandate of the TRACED Act and should be discarded as well.

Further, the Commission itself recognizes that "section 10(b) directs us to provide 'transparency and effective redress options' for both consumers and callers…."[26] The Commission cannot therefore accept the reasoning that a PCBN is unnecessary while at the same time recognize that it should provide transparency to caller. That is an arbitrary position. The Commission should explicitly refute the argument that the PCBN is unnecessary.

c) The Commission Has Acknowledged There is Strong Support for PCBN

The Commission has acknowledged that there is strong support for transparency with respect to call blocking. The *Third Report and Order* states: "There is strong support in the record for transparency and redress mechanisms, both of which are an *essential part* of any blocking regime."[27] This also demonstrates there is a need for a PCBN. Footnote 121 of paragraph 51 cites to various comments, including those from CUNA (dated Aug. 23, 2019 Reply Comments at page 3-4), which states in part on: "All blocking programs must, in addition to providing readily discoverable contact information, provide real time notification of call blocking through an intercept message or unique SIP code." Other comments cited by the Commission include those from CCA (Aug. 23 Reply Comments at 5) which states: "An irreducible minimum requirement, however, must be a notification, preferably in real-time through an intercept message and/or a SIP code, alerting callers and called parties that a call is being blocked."

[25] TRACED Act, Section 10(b)(1).
[26] *Third Report and Order*, par. 8-9.
[27] *Third Report and Order*, par. 51 (emphasis added).

Thus, by highlighting specific comments advocating for PCBN, it is reasonable to conclude that the Commission views the PCBN as a necessary and essential aspect of providing transparency to callers when blocking occurs. Considering that there is strong industry support for PCBN, and that it is viewed favorably by the Commission, it would seem to be the very definition of arbitrary and capricious for the Commission to then decline requiring this protection in its regulations.[28] Specifically, if ensuring transparency to callers is an essential part of a blocking regime, then failing to mandate this protection can only be viewed as an arbitrary decision.

Furthermore, defining an approach where service providers are provided flexibility to determine on their own whether and how to provide a PCBN appears to be arbitrary as well. If ensuring transparency is an essential party of a blocking regime, then allowing providers to opt out from providing a PCBN, or providing an ambiguous or opaque indication to callers, is not consistent with considering it an essential part of a blocking regime – namely "transparency." Allowing confusion to exist as to what information is conveyed to the caller does not meet the stringent requirement of "ensuring" transparency.

Finally, waiting for "further developments in the record"[29] does not offer a persuasive reason to ignore the TRACED Act's statutory mandate of developing a final agency action within one year from the passage of the TRACED Act. Rather, such a determination appears to be capricious. The record has shown a desire by numerous requests from the industry for a PCBN (see below) along with reasons explaining its benefits. No evidence is provided in the record that providing a PCBN would increase the number of illegal calls or cause other harms. Finally, the TRACED Act shows providing a PCBN is necessary. The Commission has no reason to wait for "further developments in the record" as a basis to disregard the statutory mandate.

D. The Commission Has Received Numerous Requests from Industry for the PCBN

The record is populated with numerous requests that some form of notification is required to be provided to the caller informing indicating their call was blocked. The

[28] See e.g., *NPRM*, par. 59.
[29] *Third Report and Order*, par. 59.

following commentators[30] all explicitly requested some form of notification and is not intended to be an exhaustive listing.

- Cloud Communications Alliance, p. 10.
- American Association of Healthcare Administrative Management, p. 5.
- American Association of Retired Persons, p. 3.
- Joint submission of: American Association of Healthcare Administrative Management, American Bankers Association, ACA International, American Financial Services Association, Consumer Bankers Association, Credit Union National Association, Edison Electric Institute, Independent Community of Bankers of America, Mortgage Bankers Association, National Association of Federally Insured Credit Unions, National Retail Federation, p. 5.
- ACA International, p. 10.
- Ohio Credit Union League, p. 1.
- Capio Partners, LLC, p. 1.
- Securus Technologies, Inc., p. 7.
- PACE, p. 4.
- Noble Systems, p. 3.
- Professional Credit, p. 2.
- PRA Group, p. 3.
- Ring Central, p. 9.
- Sirius XM, p. 7.
- TCN Inc., p. 2.
- National Consumer Law Center, p. 10.

It should be noted that these requests originate from *inter alia*, industry associations, financial institutions, healthcare providers, consumer groups, and telecom service providers. This represents a broad swath of support from industry participants. The list does not include many other commentators that highlighted the need for transparency and rapid identification and resolution of blocked calls. Such comments can be indirectly interpreted as supporting a PCBN

[30] Comments to CG Docket No. 17-59 and WC Docket No. 17-97, generally submitted on or prior to July 24, 2019.

as well. The Commission cannot state that a PCBN is not needed when there is overwhelming support for such a mechanism.

E. The Former CTOs of the Commission Have Proposed a PCBN

The Commission is cognizant of various proposals submitted to the Internet Engineering Task Force ("IETF") from former chief technical officers of the Commission, including those proposals that inform the caller of unwanted calls in a SIP environment. This includes proposals from Mr. Henning Schulzrinne for a unique SIP error code that would convey to the caller that the called party does not want the call.[31] Other proposals by Professor Dr. Eric Burger have been proposed to SIP standards forums on conveying information to the caller about unwanted calls.[32]

It is time for the Commission to mandate carriers provide both an intercept announcement and an appropriately defined SIP signaling error code so that blocked calls are unambiguously detected by callers. Doing so would be consistent with the TRACED Act which mandates the Commission to ensure, no later than one year after the date of enactment, that robocall blocking services "are provided with transparency and effective redress options for both – (i) consumers; and (ii) callers."[33] Because it is appropriate for the Commission to rely on industry standards forums to develop the appropriate SIP standards, the Commission should clearly indicate the need for a PCBN standard to be developed in a timely manner.

F. The Path Forward for Defining the PCBN

There are two common approaches for implementing a PCBN – one is an audio intercept announcement and the other is a SIP error code. The audio intercept facilitates informing a human caller, as the caller merely has to listen to the message to be informed the call was blocked and the number to use to seek redress. The SIP error code facilitates processing by digital equipment, as the error code conveys the information and the equipment can inform the user as appropriate. For

[31] https://tools.ietf.org/html/draft-schulzrinne-dispatch-status-unwanted-00. While not directly on- point for serving as a PCBN, it shows the need for additional information provided to callers as to exactly what the call encountered.
[32] See, e.g., https://tools.ietf.org/html/draft-ietf-sipcore-rejected-09
[33] TRACED ACT, Section 10(b).

example, originating equipment receiving a SIP error code can display a message to the caller, play a recorded announcement, and/or log the occurrence for reporting purposes.

Ideally, both approaches would be used to provide notification of a blocked call. Currently, one major carrier is using an intercept announcement, while another major carrier is using a SIP code.[34] It is expected that a carrier would agree to adopting a single approach consistent with what they are already doing. Thus, adopting one approach will likely be viewed favorable by one carrier and disfavored by another. The Commission should adopt both approaches of providing an intercept announcement and error code in a PCBN. This provides the greatest flexibility for the caller and ensures no one carrier is advantaged.

The Commission can establish an initial goal of requiring service providers to provide one form of notification, and then in a year or two, supplement this by providing the other form, such that both forms of notification are provided to the caller. The approach of allowing each carrier the flexibility of choosing their particular form of PCBN is not readily feasible for achieving the statutory mandate of ensuring transparency. If each carrier could elect which SIP error code to return or whether or not to use an intercept announcement, then the benefits of uniformity are lost and transparency would not be ensured. Allowing flexibility of service providers to choose their own approach would allow them to repurpose existing intercept announcements or SIP codes, providing a 'fake busy', etc. Transparency to the caller would not be achieved. The Commission should require a common, universal PCBN mechanism deployed by voice service providers.

III. REASONABLE ANALYTICS, CALL BLOCKING, AND SAFE HARBOR

The TRACED Act, section 4(c)(1)(B) mandates the Commission promulgate rules for a safe harbor, specifically:

> (B) establish a safe harbor for a provider of voice service from liability for unintended or inadvertent blocking of calls or for the unintended or inadvertent misidentification of the level of trust for individual calls based, in whole or in part, on information provided by the call authentication frameworks under subsection (b).

[34] See, e.g., Call Blocking Tools Now Substantially Available to Consumers: Report on Call Blocking, CG Docket No. 17-59, June 2020, Federal Communications Commission, pages 12 and 17.

There are two different situations described in this language. First, there is the unintended or inadvertent blocking of calls. This usually refers to blocking by the terminating service provider, which can be based on call authentication information it receives in the call. Second, there is the unintended or inadvertent misidentification of the level of trust for a call, which is the attestation level assigned by the originating carrier.

Focusing on the latter situation first, the safe harbor applies when a voice service provider blocks a call based on an unintended misidentification level of trust given to a call by the originating service provider. Thus, for example, a terminating service provider that receives a call that is incorrectly given a "C" attestation level by the originating service provider may block the call and would be covered by a safe harbor. Obviously, the terminating service provider should not be liable for blocking a call based on a mistake of another service provider. In this case, the terminating service provider blocking a call with the incorrectly determined information is predictable and deliberate based on its algorithm. That is, the algorithm performed as it was configured to do, even if the incorrect attestation level was provided to it. That still could be viewed as the application of "reasonable analytics" leading to the blocking of the call.

However, consider the former situation, when the safe harbor applies to the terminating service provider blocking a call which has a correct level of trust. For example, if the originating service provider correctly assigned a "C" level of trust to a call, and the terminating service provider blocks the call, consistent with the parameters of the algorithm, then is that inadvertent?

The Commission has adopted regulations predicating the safe harbor upon the incorporation of reasonable analytics. "We thus adopt a safe harbor for terminating voice service providers that block calls based on reasonable analytics and caller ID authentication information as described in the *Call Blocking Declaratory Ruling and Further Notice*."[35] The analytics algorithm may incorporate various other factors in deciding whether to block the call, including large bursts of calls in a short time, low average call duration, a large number of complaints, and neighbor spoofing patterns.[36] Again, the same question applies: if the algorithm blocks a call in accordance with the parameters and process defined by the algorithm, is that outcome inadvertent?

[35] *Third Report and Order*, par. 26.
[36] Id.

A. Scope of "Reasonable Analytics" Is Unclear

The Commission seeks further comment on call blocking and the application of reasonable analytics.[37] Unfortunately, the scope of "reasonable analytics" itself is a term that provides little guidance to industry or to callers. The algorithms are proprietary and there is no expectation that the details of these processes should be publicly disclosed for evaluation. Likely, every service provider would respond that every instance of a call being blocked is the application of reasonable analytics. In other words, if the algorithm resulted in blocking the call, then the outcome must have been 'reasonable' as the algorithm was designed to block the call under the defined circumstances. This is circular logic. Without a PCBN, the caller cannot provide evidence that their call was blocked, let alone by the application of "unreasonable analytics." Even with a PCBN, the caller is handicapped, because the caller does not know the other criteria which the analytics may be evaluating in determining whether to block the call.

There is a problem if the Commission does not give some objective meaning to this term. Predicating certain rights (the safe harbor) on an undefined or superfluous term ("reasonable analytics") subjects the regulation being deemed arbitrary. There must be some distinction or guidance to distinguish between "reasonable" and "unreasonable" analytics, as well as "inadvertent" versus deliberate blocking of a call.

Furthermore, service providers cannot be allowed to justify every blocking of a call as the application of reasonable analytics or arguing that if it blocked a call, it was not inadvertent. Doing so would provide them *carte blanche* ability to block calls without liability.

The TRACED Act references the provision of the safe harbor is for the "unintended or inadvertent blocking of calls."[38] The Commission has not explicitly interpreted this term, and it appears that the Commission is expecting the application of "reasonable analytics" to cover this statutory requirement. However, when an algorithm is configured to block a call under specific conditions, blocking the call is (by definition) reasonable in light of how the algorithm is defined. The algorithm is not "unreasonable" for doing exactly what it was programmed to do – the outcome appears to be intentional. In fact, every call meeting the defined criteria for being blocked, by

[37] NPRM, at par. 83.
[38] TRACED ACT, Section 4(c)(1)(B).

definition, will be blocked. Thus, it is not clear that using "reasonable analytics" implements the statutory language pertaining to addressing "inadvertent" or "unintentional" blocking.

Consequently, this calls into the question what does it mean when a voice service provider blocks a call inadvertently or unintentionally? The answer to this is gained by considering the TRACED Act's mechanisms for redress in Section 10(b). That Congress mandated redress mechanisms for erroneously blocked calls means that Congress knew that some calls will be mistakenly blocked, i.e., blocked when they should not have been, and that redress would be available to correct the situation. Thus, a call being the subject of a redress request would be an instance of an inadvertently or unintentionally blocked call.

This means that an inadvertently blocked is determined outside the scope of the analytics algorithm itself (i.e., its reasonableness) and determined from the perspective of the caller or called party. In other words, if either the caller or called party has indicates the call should not have been blocked, then there is a basis to consider the call as an inadvertently blocked call. In such cases, the service provider prior to not knowing that the call should not have been blocked is entitled to the safe harbor.

But, this raises various questions: once the service provider is informed that the call should not have been blocked, is the service provider still entitled to a safe harbor? Is the service provider excused when using analytics to block the call again (i.e., from the same calling party number)? Specifically, what happens when the caller demonstrates that the call was wanted and legal? Is the terminating service provider entitled to a safe harbor if they block future calls?

Analytics providers will point out that with spoofing, a large volume of spoofed calls may be received purporting to be from that same calling party number. Thus, it is reasonable to expect that the terminating service provider cannot promise to not block calls in the future from that number. A scammer may originate a large number of calls spoofing that number that are illegal, which a reasonable analytics algorithm would block. After all, spoofed calls may be illegal calls and it is presumed that called parties do not want to receive illegal calls. It is not feasible, in many circumstances (i.e., without call authentication), to distinguish legitimate calls from a calling party number from illegitimate calls spoofing the same calling party number. Without anything more, reasonable analytics algorithms cannot accurately distinguish between the two types. In the context of such uncertainty, "reasonableness" has value.

A terminating service provider receiving calls with "B" or "C" attested levels knows that it is possible the calling party numbers are spoofed. In fact, a "B" level indication is suggestive that number may be spoofed. Thus, blocking may be appropriate by the terminating service provider. But this framework changes once call authentication information is present.

As call authentication is deployed, a greater number of calls are expected that will be authenticated with "A" level attestation. This alters the analysis for what involves an inadvertently blocked call. The calling party may approach a terminating service provider and essentially state: "You reasonably blocked my legal and wanted calls in the past because they could not be differentiated from spoofed calls from scammers, but now my calls are fully authenticated. You know these calls are not spoofed, you know that they are legal, and you know that the called party wants to receive such calls. These calls should not be blocked."

So the question arises: after a caller demonstrates to the terminating service provider the their calls are wanted and legal, and the calls are received by the terminating service provider as "A" level authenticated calls, is the terminating service provider entitled to a safe harbor if they continue blocking such a call? Stated another way, is it an application of "reasonable analytics" to block a call that is fully authenticated and known by the service provider that it should not be blocked?

This is not a hypothetical question. In fact, many enterprises would view this as a solution to eliminate potentially erroneous blocking. Many financial institutions, debt collectors, alarm companies, and other enterprises are likely prepared to indicate to service providers the calling party number they use to contact their customers along with evidence that the called parties consented to receive such calls and that the calls are legal. Many enterprises would do so if they had the expectation that once call authentication is deployed, their calls will no longer be blocked. While there may be issues in resolving erroneously blocked calls in the early stages of call authentication deployment, enterprises would find that the scope of the problem would diminish in times as more and more of their calls are receiving "A" level authentication.

Enterprises would consider that once the terminating service provider is informed that a fully authenticated "A" level call is shown to be wanted and legal, then it should not be reasonable for an analytics algorithm to block their call. In such cases when the analytics program blocks a fully attested call after the service provider knows the call is wanted and legal, the analytics

algorithm operated exactly as it was programmed to under those circumstanced. This means that the terminating service provider is not entitled to a safe harbor because the call blocking was, in effect, intentional.

Obviously, this has significant ramifications for service providers blocking calls. First, a situation is clearly defined when the safe harbor can be lost for a service provider. Before, under the Commission's regulations, it was not clear when that could occur. Second, when coupled with a PCBN, the caller is aware of every blocked call, and mistakes are verifiable. The existence of a blocked call is not masked through some opaque call treatment.

This does not mean that fully authenticated calls cannot be blocked, nor that they would not be processed by an analytics algorithm. It only means that such calls would not be *automatically* blocked using analytics. Rather, analytics algorithms could automatically flag fully authenticated calls as warranting manual investigation. It is an unusual situation when a fully authenticated call that has been shown to be legal and wanted by the called party and is subsequently suspected as illegal. There are examples when this can happen. For example, an enterprise's can be PBX hacked and originate fully authenticated but illegal calls. Or, spammers may engage in "snowshow spamming."[39] In summary, "reasonable analytics" could be used to identify fully authenticated calls that should be investigated, but humans would institute blocking after such investigation.

The Commission indicated in the *Third Report and Order* that fully authenticated calls could be blocked using reasonable analytics. "If the terminating voice service provider has identified that calls with "A" attestation previously originating from that number are nevertheless illegal or unwanted *based on reasonable analytics*, they may block those calls despite the attestation level." [40] This statement does not address whether the safe harbor applies to the terminating voice service provider when using reasonable analytics to block an "A" level attestation call *after* the caller has demonstrated that calls from those numbers are legal and wanted. Callers will argue that once the terminating service provider knows the calls are legal and wanted, then fully attested calls

[39] This is when fully authenticated numbers are used in low volumes for spamming. See, e.g., TNS Comments, page 5.
[40] *Third Report and Order*, par. 31 (emphasis added).

being blocked are being blocked by the analytics algorithm as deliberately (or negligently), not inadvertently.

The Commission should clarify that a terminating voice service provider using analytics to block a fully attested *call after being aware the calls are wanted and legal* does not give the terminating voice service provider a safe harbor. The terminating service provider bears the burden to 'get it right' with respect to blocking a fully attested call after they have been notified.

The TRACED Act's language makes clear that a safe harbor is not to be granted for all blocked calls. Specifically, only a subset of calls, those unintended or inadvertent blocked calls warrant a safe harbor.[41] The TRACED Act clearly mandates redress to the caller for erroneously blocked calls. The expectation of receiving redress is that upon confirming it was erroneously blocked, the service provider would not continue to block such calls. This raises the question of whether Congress intended to grant voice service providers a safe harbor when they continue to block such calls after agreeing to provide redress.

The Commission should also clarify that the terminating service provider can avoid the risk of losing a safe harbor by adopting a policy of not using analytics to block fully attested calls. The terminating service should be covered by the safe harbor if they manually investigate such suspicious calls and then decide to institute blocking. In that case, it is human judgement, not algorithmic analytics involved, in making the determination to block calls from that number. However, this requires the voice service provider demonstrate that it is their policy to not block fully attested "A" level calls without first investigating them.

This approach is similar in some ways to the approach adopted by the Commission for blocking calls for bad-actor service providers.[42] Voice service provider may block such calls after being informed that upstream voice service providers are originating suspicious calls. Those upstream service providers are notified, and then given a limited time to take effective mitigation measures. Then, the call is blocked. This involves the application of human judgement at some point during the process in determining calls from the originator or service provider should be blocked.

[41] And, of course, those calls blocked based on a misidentification of the level of trust.
[42] See generally, *Third Report and Order,* par. 35-45.

B. The Regulations Do Not Clarify How Redress Is Available to Callers

The above description focuses on the ramifications after a caller informs the terminating voice service provider of an allegedly erroneously blocked call. The current form of the regulations suggest (upon initial review) that the caller can avoid having calls blocked by merely by make a credible claim of erroneous blocking. Specifically:

> We further require that when a caller makes a credible claim of erroneous blocking and the voice service provider determines that the calls should not have been blocked, a voice service provider must promptly cease blocking calls from that number unless circumstances change.[43]

It is unclear what constitutes a credible claim, but it may entail providing evidence that the call is legal and wanted. So, once the caller has provided evidence that the call is wanted and legal (and presuming the call is fully attested as an "A" level via call authentication), can the caller then presume that the call will not be blocked?

The Commission's regulations, however, provide a qualification at this point:

> 56. Consistent with what we permitted in June 2019, consumers may choose, either via opt in or opt out consent, to have their terminating voice service provider block categories of calls that may include legal calls. In these cases, terminating voice service providers are not obliged to cease blocking such calls merely because the caller claims they are legal. Rather, a terminating voice service provider's analysis should hinge on whether the disputed calls fit within the blocking categories to which their customers have consented.[44]

The regulations explicitly indicate that demonstrating the call is legal is not sufficient. Presumably, evidence must be provided showing the call is also wanted. However, the terminating voice service provider merely has to respond to the caller that the disputed call fits within a category of calls which their customers have consented to be blocked and therefore is not wanted.

Such a category could be, e.g., "spam" or "robocall." It is readily evident that there is no objective criteria agreed to by industry as to what is constitutes "spam" or a "robocall." There is no obligation under the regulations for the service provider to disclose how they define what constitutes "spam." Indeed, a service provider publicly defining the criteria used to block such

[43] *Third Report and Order*, par. 55.
[44] *Third Report and Order*, par. 56.

calls as spam risks informing scammers how to evade that criteria. So, it appears the Commission is allowing a service provider to simply reject any erroneous blocking request as falling into a category which the called party has consented to be blocked. Absent that approach, the service provider can merely argue that "circumstances have changed" which is another nebulous reason as to why no redress is available.

Service providers would likely counter that this is an extreme view and unreasonable. But, under the Commission's regulations, callers could have their calls repeatedly blocked, and service providers merely have to respond that: 1) their analytics are reasonable, 2) that the call is of the type the consumer wants blocked, or 3) circumstances have changed. Consequently, the Commission's regulation requiring service providers to respond to an erroneous blocking allegation may provide no redress to callers that provide evidence their calls are wanted and legal.

C. An Alternative for Reasonably Accommodating Emergency Calls

The above approach where fully authenticated "A" level calls are not blocked using analytics means these calls are treated as a presumptively legal, wanted calls and are not blocked. Concerns of consumers being flooded with unwanted calls are not warranted. If the call is an unwanted, but legal telemarketing call, the called party can request to be added to the caller's do-not-call list. If the call is an illegal telemarking call or a scam call, the called party can report the caller to their service provider (see Customer Originated Trace below). Bad actors originating calls using fully authenticated numbers, even with a low volume of calls, are quickly identified and with the Customer Originated Trace feature, they can be quickly reported. At that point, the burden should be on service providers and regulators to stop the calls of bad actors. Legitimate callers whose calls are fully authenticated should not bear the burden.

This approach of not blocking fully attested "A" level calls will apply to emergency calls that have "A" level authentication. Many of these emergency calls are likely to originate in urban areas where call authentication technology will be introduced initially. Thus, many emergency calls will have "A" level attestation by June 30, 2021. Further, as time progresses, there should be wider deployment of call authentication technology such that there will be fewer emergency calls that do not have "A" level attestation. The approach of not blocking fully attested "A" level calls

means that the scope of the problem of how to handle unauthenticated emergency calls reduces going forward in time.

Voice service providers are expected to use "reasonable care, including making all reasonable efforts to avoid blocking emergency public safety calls." Absent this approach of not automatically blocking fully attested calls, voice service providers may be expected to maintain secret 'whitelists' of emergency numbers, which are checked by analytics algorithms, so that such calls are not blocked. This approach has a number of issues, least of which is an administrative burden. Further, scammers can easily guess what these emergency numbers are, and spoof them to avoid blocking. Once call authentication is widely deployed, scammers spoofing these numbers (whether they spoof emergency or other numbers) will be identifiable.

Consider the situation of the alarm industry. In this case the consumer definitely wants to receive the calls and they are legal calls. Setting aside the harm that can arise if even a single call is blocked, assume that the alarm vendor is informed via a PCBN that a call is blocked. They will immediately seek redress with the voice service provider. Upon demonstrating that calls from the originating number are wanted and legal, the voice service provider agrees to not block future calls. Assuming the calls are fully authenticated with "A" level attestation, what if the voice service provider continues to block such calls at various times? Can the voice service provider merely argue it was because of changing circumstances? Is the voice service provider entitled to a safe harbor after explicitly acknowledging that the calls are wanted and legal, and indicated they will not be blocked? In this case, the voice service provider has the option of: 1) bear the risk of subsequent blocking a fully attested "A" level call using analytics (meaning there is no safe harbor for blocking after being notified), or 2) avoid that risk by not using analytics to block a fully attested call. As stated, analytics can be used to flag such calls for manual investigation of such calls, which can then be blocked. Presumably, the terminating voice service provider would discover during investigation that the calls originate from an alarm vendor and would proceed appropriately in deciding whether to institute blocking.

D. Blocking Based on Call Authentication Status

The Commission seeks comment on whether blocking based on call authentication status alone would ever be justified.[45] There is a situation where blocking may be appropriate that is largely based call authentication and does not involve the application of analytics. For example, a service provider may know that certain emergency numbers are not to be blocked by maintaining a list of emergency numbers. The list may further reflect that the calling party numbers are normally fully attested by the originating service provider. In many instances, emergency call originators originate their calls in urban areas served by service providers that have upgraded their equipment to authenticate calls. Thus, the presence of a call using the emergency number but where the call authentication is "B" level or "C" level is highly suspect. Presumably, such a call is more likely the result of a scammer spoofing an emergency number as opposed to the originating service provider somehow derogating the call authentication level. Thus, a voice service provider should not expect to see certain numbers that are variously authenticated as "A","B", and "C" traversing their networks. In another example, some carriers may have implemented call authentication in their own network. Receiving a call, which they know originated in their network, means that the call should have been fully authenticated. If the call contains a number that originated in their network that is not fully authenticated, then that also suggests a suspicious call. This situation is recognized by the Commission in paragraph 31 of the *Third Report and Order*.

E. Summary of a Framework for Call Blocking/Safe Harbor/Redress

To recap, a terminating service provider should be:

1) Granted a safe harbor for using reasonable analytics for blocking unauthenticated calls or calls with "C" or "B" level attestation. Such calls may be spoofed or legitimate, and analytics can sort these out.

2) Should not be granted a safe harbor for using analytics (reasonable or otherwise) when blocking an "A" level authenticated call, after the caller or called party has indicated the call is wanted and legal. Essentially, once the service provider knows a fully authenticated call

[45] *NPRM*, at par. 83.

should not be blocked, then there are liable for using analytics to automatically block a call that has not been investigated.

3) Should be granted a safe harbor for blocking a call having an "A" level authentication level (using reasonable analytics or otherwise) after having investigated the circumstances and determining the call is suspicious.

4) There is one other option, which is compatible with the Commission's existing regulations.[46] This option allows preservation of the regulation allowing a provider to block an "A" level call using reasonable analytics. Specifically, should a voice service provider choose to use analytics to block a fully attested "A" level call, then they are granted a safe harbor on the condition that the caller or called party has *not* indicated the call is wanted and legal. Essentially, the service provider is granted a safe harbor for blocking a suspicious "A" level call only absent of being informed the call is wanted and legal. However, once redress is sought and the call is legal and wanted, then voice service provider loses their safe harbor if analytics then blocks the call.

IV. CUSTOMER ORIGINATED TRACEBACK REQUESTS

The Traceback Consortium promises to be an effective tool in the arsenal to combat illegal calls. That mechanism is useful for stopping large scale illegal callers and that body is geared for information sharing with the Commission and other carriers. However, the Traceback Consortium does not appear suited for direct consumer interaction. Notwithstanding the effectiveness of the Traceback Consortium, the Commission should develop some form of consumer-oriented mechanism for reporting unwanted or illegal calls to their service provider.

Some voice service providers in the past have offered a customer originated trace ("COT") that is associated with Custom Local Area Signal Services ("CLASS") that could be invoked using

[46] An alternative involves a change to the Commission's regulations. Specifically, a sentence in paragraph 31 of the *Third Report and Order* to changed to read: "If the terminating voice service provider has identified that calls with "A" attestation previously originating from that number are nevertheless illegal or unwanted based on investigation identified by using reasonable analytics, they may block those calls despite the attestation level." This reflects that "A" level calls may be blocked after manual investigation (which may be triggered by using reasonable analytics) determines the calls are illegal or unwanted.

a vertical service code; specifically "*57". The COT could be invoked after a call for purposes of reporting a suspicious call.

The application of this (or some other) code could be adapted in a STIR/SHAKEN environment to allow a consumer to signal to their service provider that the call was unwanted and/or illegal. This would not necessarily result in automatically blocking calls from that number, since such allegations may be incorrect. However, this could be a mechanism to allow a called party to report a calling party number as potentially warranting investigation. These requests could be collected and analyzed by service providers to identify potential callers to investigate or could be reported to the Traceback Consortium if a threshold level is reached. As such, it would be useful to detect "snowshoe spamming." [47]This would be a consumer- oriented mechanism for quickly receiving consumer input to identify potential originators of scam or illegal calls. Thus, assuming that fully authenticated "A" level calls are not blocked using analytics, analytics could analyze such requests to identify potential situations to investigate. To date, there does not appear a consumer-oriented mechanism for consumers to report unwanted calls in a consistent, easy manner to their service provider.

The Commission seeks comments on mechanisms that could be used to fulfill Section 7 of the TRACED Act, which would "help protect a subscriber from receiving unwanted calls or text messages from a caller using an unauthenticated number."[48] The first step in protecting unwanted calls to a subscriber is to know from the subscriber when unwanted calls are received. Currently, there does not appear a universal, widely known mechanism which callers can be directed to invoke for purposes of identifying unwanted voice calls.

This could also be another tool used by service providers to gauge the effectiveness of their call blocking services. That is, a relatively low level of such customer requests reflects that consumers are not receiving an excess of unwanted calls. A voice service provider receiving such requests would know if the calling party number corresponds to one of their own customers and could investigate internally. Otherwise, the voice service provider could forward such information

[47] See, e.g., TNS Comments at page 5, describing a practice of using low call volumes on a plurality of authenticated numbers to originated scam calls.
[48] *NPRM*, par. 88.

to the originating carrier for investigation. A high number of such customer requests, particularly if they identify a common calling party number, can be useful to identify potential bad actors.

Presently (i.e. pre-call authentication), there are informal mechanisms used by carriers and service providers to relay requests to originating providers for investigation of suspicious calls. These frequently involved called parties complaining to their carrier about calls from spoofed numbers, which necessitates the originating carrier investigating their customer associated with that number. In many cases, their customer is not, in fact, originating the calls. Currently, it is presumed that individual called parties somehow notify their respective carriers in some manner, and this may involve contacting their providers' customer service representatives. This approach is expensive for the service provider in that it consumes human resources, but it likely is the only known approach that customers are aware of for seeking redress. The automated customer originated trace could provide a lower cost, alternative approach.

V. BLOCKED CALL LISTS

The Commission seeks comments on the provision of blocked calls lists to consumers.[49] In principle, consumers should be provided information about calls that are blocked. Such a list is useful for the consumer to confirm whether a call from a given number was previously blocked. However, the Commission should be aware that such a list, by itself, does not provide a solution to the problem of whether "a consumer may not know that they are missing calls they would prefer to receive."[50]

It is not reasonable to presume that consumers will proactively check as to whether a wanted call was blocked by proactively reviewing the call blocking list. A consumer viewing, e.g., a list of 50 telephone numbers that were blocked would not know which of those numbers were associated with calls that were wanted versus unwanted. It is possible that an unrecognized number on that list corresponds to a call that was very much wanted. It is unreasonable to presume that a consumer would recognize the source of the numbers or investigate unrecognized numbers to

[49] NPRM, par. 110 and 111.
[50] NPRM, par. 111.

ascertain whether the call was wanted or not. Practically speaking, this would entail the consumer calling back the number to ascertain why the call was initially made.

Frequently, the caller will have supplemental information indicative of whether the consumer wants the call. For example, the caller may have been requested by the consumer to receive important notifications – such as alarm notifications. Hence the caller may know that the call should not be blocked. This is another reason why a PCBN should be provided to the caller, so that if the call is blocked, the caller will know immediately and can contact the caller to confirm the situation. The caller may even request the consumer to 'unblock' their number on their blocked call list. It is safe to presume that if the consumer seeks redress from their service provider to unblock a number, this will be completed with greater certainty and speed by the voice service provider than if the caller seeks redress for an allegedly erroneously blocked call.

VI. CALL LABELING

The Commission asks for comment regarding potential regulation of call labeling.[51] Many callers have complained about mislabeling of their calls. Some labels are provided by service providers acting as agents to VoIP service providers and other labels are provided by third party mobile applications that are not affiliated with the voice service provider. Thus, some entities are under the regulatory authority of the Commission, whereas others appear outside.

The topic of labeling is an area that the Commission should be cautious in regulating. Developing regulations regarding the use of call labels is an open invitation for first amendment challenges to government regulation of speech. Those clamoring for regulation are primarily callers whose calls are being mislabeled (and presumably, not the service providers). While those requesting regulation may not be currently happy with the results of the labels assigned to their calls, it is far from certain whether they would be any happier with the results of labeling based on regulations covering this area. It is safe to presume that service providers are not seeking regulation and would object to such regulations.

In considering whether the Commission should regulate this area it is useful to review why call labeling developed. Call labeling arose largely to address the onslaught of spoofed and scam

[51] NPRM, par. 109.

calls. Because illegal telemarketing or scam calls could hide their identify by spoofing and generate millions of calls, consumers could no longer trust the calling party number and could not distinguish wanted calls from the numerous unwanted calls. Furthermore, without an accurate calling party number, any calling name provided was not accurate. Thus, the calling number and calling name were rendered useless. So, an ecosystem arose in which third party providers would independently assess the nature of the call and provide a label with the call. Soon, these providers partnered with voice service providers. Consumers found that a broad label, even one that characterizes the call as "robocall" or "spam," was better than nothing.

The development of call authentication was intended to identify spoofed telephone numbers. It can be expected the deployment of call authentication will lead to greater percentage of callers having their numbers authenticated. It can be further expected that called parties will be informed at some point in some manner of the authentication status via a display or other indicator on their phone. This, coupled with traceback efforts, (and the above mentioned customer originated trace) means that illegal telemarketers and scammers will be isolated and identified more quickly. Call authentication has a goal to restore trust in telephone calls.

Industry is also working on a related technology known as enhanced calling name. This also has a goal is to restore trust, but this is targeted at the calling name for fully authenticated calls. This service provides greater flexibility by allowing the caller to indicate additional information with a call, such as additional contextual information. Consequently, called parties can expect to see trusted information about the caller and can thus better determine whether they want to answer the call. Certainly, authenticated enhanced caller information is more useful than a generic "spam" or "robocall" label.

It should be the goal of the Commission to ensure consumers can trust caller ID information, whether it just be the telephone number and/or calling name and/or enhanced contextual information. Given this goal, the Commission should evaluate whether the caller will rely more on the enhanced calling name information or a call label attached to the call. Likely, the called party will find the authenticated number, associated name, and context of a given call more useful and reliable than a label. If this is the likely expected outcome in a few years, then a generic label attached by a service provider will become either superfluous or of little value when the call

is provided with enhanced calling name information. That means the Commission's regulations governing call labeling will be obsolete.

Given that labeling may be rendered obsolete as an outcome of restoring trust back into the telephone network, the Commission should think twice about entering the thicket of regulating call labeling and all of its associated issues. Such regulations are likely to be highly contested and frequently litigated. There does not appear to be a clear path to success in regulating this area. The Commission would be better served to advance deployment of enhanced calling name services and let market forces render call labeling obsolete.

VII. CONCLUSION

The Commission should complete requirements for voice service providers blocking calls to provide a per-call blocking notification ("PCBN") to the caller. This should comprise both an audio intercept announcement and an appropriately defined (i.e., unambiguous) SIP error code. Doing so allows the Commission to meet a number of its mandates under the TRACED Act. Failing to do so places the Commission in an awkward position, as there are no persuasive reasons why it should not have done so and is inconsistent with its own admission that transparency to the caller is essential and requested.

The Commission should clarify its regulations as to when fully authenticated calls can be automatically blocked using analytics. Specifically, once calls are fully authenticated, and a caller informs the voice service provider that their calls were erroneously blocked, the Commission should clarify whether the voice service provider is entitled to a safe harbor if it knowingly blocks that call. For clarity and for consistency with the TRACED Act, the Commission should clarify that callers who have sought redress for blocking a fully attested "A" level call can expect that their fully attested "A" level calls will not be automatically blocked again. Such calls can be blocked, but only after manual investigation has determined it to be appropriate. At that point, the voice service provider is provided with a safe harbor if the blocking was inadvertent. Thus, the judgement for instituting blocking is based on human judgement, not analytics.

Respectfully submitted on August 31, 2020

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