Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

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

REPLY COMMENTS OF TELTECH SYSTEMS, INC.

Mark Del Bianco
Law Office of Mark C. Del Bianco
3929 Washington St.
Kensington, MD 20895
301-602-5892
mark@markdelbianco.com

Meir Cohen
Co-Founder and CEO
Ethan Garr
Senior Vice President for Strategic Growth
TelTech Systems, Inc.
101 South Broadway
South Amboy, NJ 08879

August 22, 2019

Table of Contents

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

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

Introduction

TelTech Systems, Inc. ("TelTech") submits these reply comments in response to the Third Further Notice of Proposed Rulemaking ("*Third FNPRM*") in the above captioned dockets and in reply to the comments filed in response thereto.[1]

TelTech creates unique and innovative mobile communications applications and services that protect consumers' privacy and allow its customers to control the who, what and when of their voice communications.[2] Most notably for purposes of this proceeding, TelTech offers RoboKiller, a mobile application that identifies and blocks unwanted calls from telemarketers and other unwanted robocalls through the use of proprietary algorithms and analytics.

TelTech has a long history of working with Congress, the Commission and law enforcement to address telecommunications laws and regulations. In 2009 and 2010, for example, TelTech worked with staff of both the House and Senate to develop what became the Truth in

[1] *See Advanced Methods to Target and Eliminate Unlawful Robocalls*; *Call Authentication Trust Anchor*, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, FCC 19-51 (2019). Paragraphs 22-44 of the *Third FNPRM* are referred to as the "*Declaratory Ruling."*

[2] In addition to RoboKiller, TelTech has developed and offers TrapCall, NoMoreVoicemail and Phone Lookup Pro. TrapCall is a mobile service that among other features allows a user to unmask blocked caller ID, block unwanted calls, and identify unknown numbers. NoMoreVoicemail is a service that allows users who no longer wish to receive voicemails to prevent caller access to the voicemail box on their mobile phone service. Phone Lookup Pro is an iOS mobile application that allows users to lookup caller name and information for any phone number.

Caller ID Act of 2010. TelTech subsequently participated in the Commission rulemaking that resulted in the regulations implementing the Act.

TelTech also has a long record of proactive co-operation with law enforcement. In addition to responding annually to dozens of subpoenas and search warrants from U.S. law enforcement, TelTech has co-operated through international legal channels with law enforcement agencies from numerous other countries. TelTech has also provided training sessions for U.S. law enforcement and prosecutorial personnel on the mechanics of caller ID spoofing and on fraudulent and other illegal uses of caller ID spoofing.

TelTech fully supports the efforts of the Commission and industry to protect consumers against illegal and unwanted robocalls. The *Declaratory Ruling* and other recent Commission actions on robocalls are positive steps towards solving the problem.

Summary

The Commission should not adopt its proposal to create a safe harbor allowing voice providers to block calls that fail Caller ID authentication under the SHAKEN/STIR framework. In fact, the Commission probably does not have the power to require or create such a safe harbor for network blocking because so many legal calls would inevitably be blocked. Absent substantial future changes to the SHAKEN/STIR framework, such a safe harbor would violate the Communications Act mandate that the Commission ensure that legal calls are completed.

Instead, the Commission should focus on and encourage the further development of analytics-based frameworks for blocking illegal and unwanted calls. Development of a safe harbor for blocking programs based on reasonable analytics would be feasible and desirable today. If the Commission does not agree, it should at least closely monitor technological developments in this

area. When it believes the levels of accuracy warrant, it should move expeditiously to provide a safe harbor for analytics-based call blocking at the network level.

TelTech believes that the Commission should facilitate or implement a centralized Critical Calls List for certain emergency calls that should never be blocked. In TelTech's experience, identifying those calls and creating a Critical Calls List is a difficult and resource intensive process. Moreover, it is crucial to keep in mind that as the scope of such a list expands, the risks of misuse and breach multiply. Finally, TelTech offers comments on the issue of white lists raised in the *Third FNPRM.* TelTech's comments are based on its years of experience in developing and operating individual, customer-specific white lists for its mobile apps.

I. The Commission Should Not Create A Safe Harbor for Call Blocking Based Solely On Failure of Authentication under SHAKEN/STIR

In the *Third FNPRM,* the Commission sought comment on whether it should create a safe harbor for voice service providers "that choose to block calls (or a subset of calls) that fail Caller ID authentication under the SHAKEN/STIR framework."[3] If it were to create such a safe harbor, the Commission would have to conclude, either implicitly or explicitly, that call blocking based solely on a failure of SHAKEN/STIR authentication is both "based on . . . reasonable analytics " and a reasonable practice under Sections 201 and 202 of the Communications Act.[4] Any such conclusion would be arbitrary and capricious given the evidence in the record of this proceeding.

The SHAKEN/STIR framework contemplates three levels of attestation based on the originating voice provider's level of confidence that the calling party is authorized to use the

[3] *Third FNPRM* ¶ 48. There is some ambiguity in this section of the Third FNPRM, which originally refers to call blocking programs that generally "take into account whether a call has been properly authenticated under the SHAKEN/STIR framework." ¶ 46 (emphasis added). If the Commission is considering a safe harbor for multi-factor call blocking analytics programs in which failure of SHAKEN/STIR authentication is but one input, TelTech would support such an approach, as discussed in Part II below.

[4] 47 U.S.C. §§ 201(b) and 202(a).

number that would be presented in the Caller ID. The proposed safe harbor would not allow blocking if there is any level of attestation.[5]

The main problem with the Commission's proposal, as many commenters have pointed out, is that many types of calls that are perfectly legal can "fail" SHAKEN/STIR protocol authentication. SHAKEN/STIR authentication was never intended to serve as a proxy for the legality or illegality of calls, and it is not designed to and does not enable a service provider to determine the intent of a caller. Thus, authentication results under SHAKEN/STIR are by themselves unreliable in identifying illegal and unwanted calls and will remain so.[6] A fully authenticated and verified call can be made by a bad actor, and an unauthenticated and un-verified call can be placed by a legitimate caller. SHAKEN/STIR is essentially one signal indicating a call's validity. As such a signal, it can at best assist call analytics tools and systems in making decisions. By itself, and even if universally implemented, SHAKEN/STIR will never enable an acceptably accurate or safe call blocking decision.

Moreover, during the initial years of SHAKEN/STIR implementation there will be a substantial percentage of valid calls where there is no authentication.[7] The reasons for the lack of authentication will often have nothing to do with the legality of the call. Rather, the causes for failure will be structural, technical or economic. As a result, there will be numerous participants in the voice services ecosystem whose calls cannot be authenticated under SHAKEN/STIR as it presently exists.

---

[5] *Third FNPRM* ¶ 50.

[6] First Orion Comments at 3-6 and 15 ("First Orion Comments").

[7] See, *e.g.,* Comments of the American Association of Healthcare Administrative Management, at 4-5 ("AAHAM Comments"); First Orion Comments at 4-6; Comments of INCOMPASS, at 7-10 ("INCOMPASS Comments").

The structural problems arise from the limited scope and nascent status of the SHAKEN/STIR project. The framework presently is only designed to apply to voice service providers and to operate on IP networks. Its governance structure and a number of its essential standards are still under development.[8] Moreover, SHAKEN/STIR is not yet an international initiative. European and other overseas voice service providers will not be part of the system for years, which will further limit the number of calls being authenticated.

The most important domestic group presently excluded from the framework is smaller (mainly rural carriers), who due to technical network issues - many are still operating TDM-based networks- and economic factors - particularly the costs of SHAKEN/STIR implementation- will not be able to implement SHAKEN/STIR for perhaps years.[9] In addition, the SHAKEN/STIR framework does not presently incorporate other types of non-carrier entities, including over the top (OTT) voice services providers and enhanced service providers who serve enterprise customers.[10] Similarly, the framework will not be implemented by large enterprises for years, due to the need for further development of the protocols to enable enterprises to sign their own SHAKEN/STIR certificates.[11]

Even if the majority of unauthenticated calls are illegal, a measurable and (at least at present) potentially substantial portion of the unauthenticated calls will be legal calls. For example, a small percentage of false positives among billions of blocked calls would equate to

[8] See, *e.g.*, VON Comments at 2-3.
[9] See, *e.g.*, Comments of WTA - Advocates for Rural Broadband, at 3-6 ("WTA Comments") and NTCA Comments at 3-10.
[10] Comments of Cloud Communications Alliance at 5-7 ("CCA Comments") and Comments of Telnyx LLC at 1-2 ("Telnyx Comments").
[11] See, *e.g.*, CCA Comments at 2-4, 5-7; Telnyx Comments at 1-2.

millions of blocked legal calls.[12] The misidentification of so many legal calls simply because they lack authentication is a presently insurmountable problem with SHAKEN/STIR. The number of incorrectly blocked calls would be so great for the foreseeable future that such call blocking would violate the Communications Act's requirement that legal calls be completed.[13]

Perhaps when there is near-universal implementation of SHAKEN/STIR, reconsideration of whether to allow call blocking based largely on failure of SHAKEN/STIR authentication might be appropriate. But that time is far off.[14]

There are several other factors counseling against the adoption of SHAKEN/STIR call blocking now. Most importantly, it will expand the existing incentives and opportunity for anti-competitive conduct by the large carriers, who will be the first to implement SHAKEN/STIR. They will also have the greenlight to block calls from enhanced service providers, enterprise users and the customers of smaller voice communications providers that have not adopted SHAKEN/STIR, in order to cause the enterprises and customers of the enhanced service and smaller voice communications providers to move to the large carriers' voice services.

Finally, premature adoption of blocking based solely on SHAKEN/STIR authentication would lock in place a partial solution to the robocall problem that will inevitably block many emergency calls. Adoption of this simplistic approach would also discourage the competition necessary to find new and creative solutions to the ever-evolving robocall problem. As the

---

[12] *Third FNPRM* ¶ 48. The Commission seemed to give this crucial point short shrift when it stated that it "would expect the vast majority of calls blocked in such circumstances to be illegitimate and call-blocking programs targeting such calls to be deserving of safe harbor."

[13] Therefore, there is no reason for the Commission to attempt to measure now the costs and benefits of allowing such blocking. Were it to do so, the Commission would have to balance the monetary benefits it calculated in the *Third FNPRM* against the monetary and non-monetary costs to consumers from false positives. Many of these costs are substantial and difficult to quantify. For examples of the types of harms that ought to be considered, see, **e.g.,** Comments of Credit Union National Ass'n, at 10-11 ("CUNA Comments") and Comments of Numeracle, Inc. at 5 ("Numeracle Comments").

[14] See, *e.g.*, WTA Comments at 3-6; CCA Comments at 2-9.

Commission recognized in the *Third FNPRM, "*limiting opt-out call-blocking programs to rigid blocking rules that prescribe in detail when a voice service provider may block . . . could enable callers to evade blocking, and could impede the ability of voice service providers to develop dynamic blocking schemes that evolve with calling patterns."[15]

For all these reasons, TelTech believes that at present the Commission cannot authorize network-wide blocking based solely on failure of SHAKEN/STIR authentication.[16] There are serious doubts that, even with suitable modifications in SHAKEN/STIR's scope, development and implementation, the framework will *ever* be able to sufficiently accurately identify illegal calls to justify its use as the sole basis for a network-wide blocking policy.[17] Moreover, it was never designed to, and cannot, accurately identify unwanted calls.[18] However, the Commission need not address these issues today. It is sufficient to recognize that any form of network-wide blocking based on a failure of SHAKEN/STIR authentication cannot be implemented.

Given that the Commission cannot at this time require or even permit network-wide call blocking based solely on a failure of SHAKEN/STIR authentication, the answer to the question of whether the Commission should create a safe harbor for voice providers implementing such blocking is necessarily "no."[19]

II. The Commission Should Consider Creating a Safe Harbor for Network-wide Blocking Based on Reasonable Analytics

In the *Declaratory Ruling* (at ¶ 33), the Commission clarified "that voice service providers may offer opt-out call-blocking programs based on any reasonable analytics designed to identify unwanted calls." However, the Commission did not follow up by seeking comment in the *Third*

[15] *Third FNPRM ¶ 33 (citations omitted).*
[16] See, *e.g.*, Comments of WTA - Advocates for Rural Broadband, at 3-6 ("WTA Comments"); USTelecom Comments at 7-8.
[17] See also VON Comments at 2-3.
[18] See USTelecom Comments at 6-8.
[19] *See Third FNPRM* ¶ 46 and Comments of *ACT* - The App Association at 5-6.

FNPRM on whether it should create a safe harbor for such call blocking programs. Whatever the reason for this disconnect, TelTech agrees with those commenters who contend that any safe harbor that the Commission may create should only allow carrier-based opt out blocking based on "reasonable analytics" that incorporates numerous factors such as those identified in the *Third FNPRM*.[20]

Such an approach makes far more sense than the proposal to create a SHAKEN/STIR safe harbor on which the Commission sought comment. Any analytics-based system - and certainly those offered by established firms such as Transaction Network Services, First Orion and TelTech - will always be more accurate than the simplistic SHAKEN/STIR authentication test.[21] Most importantly, any analytics-based system will have significantly fewer false positives than the SHAKEN/STIR authentication test. Moreover, the use of artificial intelligence techniques allows the accuracy of analytics-based systems to remain at a high level even as bad actors are constantly changing their robocall tactics.

Therefore, the Commission should focus on and encourage the further development of analytics-based frameworks for call blocking.[22] If it is not prepared to propose a safe harbor for analytics-based programs at this time, it should closely monitor technological developments in this area and when it believes that the levels of accuracy warrant, should provide a safe harbor for

[20] The *Third FNPRM* contemplates that providers will be able to reliably and reasonably identify illegal calls by evaluating "a combination of factors, such as: large bursts of calls in a short timeframe; low average call duration; low call completion ratios; invalid numbers placing a large volume of calls; common Caller ID Name (CNAM) values across voice service providers; a large volume of complaints related to a suspect line; sequential dialing patterns; neighbor spoofing patterns; patterns that indicate TCPA or other contract violations; correlation of network data with data from regulators, consumers, and other carriers; and comparison of dialed numbers to the National Do Not Call Registry." ¶ 35.

[21] *See, e.g.,* NTCA Comments at 12-13.

[22] *See* First Orion Comments at 14.

analytics-based call blocking at the network level. Such blocking could be based on a variety of reasonable analytics, including but not limited to those identified in the *Third NFPRM*.[23]

III. Additional Issues Relevant for Any Effective Safe Harbor for Network-wide Blocking

The *Third FNPRM* (at ¶¶ 59-66) identified a number of crucial issues that must be addressed before a safe harbor for any type of carrier-based blocking can be effectively implemented. TelTech has substantial experience with two of these issues - developing a critical calls list for non-blockable numbers and developing and maintaining both customer- and network-based white lists. TelTech offers the following comments based on this experience.

A. Implementing A Critical Calls List

TelTech agrees with the Commission that certain emergency calls must never be blocked. But in TelTech's experience, identifying those calls and creating a Critical Calls List is a difficult and resource intensive process. There are no national compilations of emergency numbers, nor any system to collect such numbers, and not even any agreement on what constitutes an emergency number. Once the universe of critical numbers is defined, just compiling a complete list will be difficult and time-consuming. Updating the list will require constant effort. Moreover, expanding the "do not block" concept to cover other categories of calls beyond 911-type emergency calls greatly complicates the task. Such an expansion would multiply the necessary effort exponentially.

The initial problem is that someone has to decide what types of entities and which numbers should be on a Critical Calls List. For example, even if the decision is that only "emergency numbers" will be included, there is no clear definition of what would constitute an emergency number. There is apparently universal agreement that outbound calling and callback numbers for

[23] See *Third FNPRM* ¶ 35 and West Telecom Comments at 14-16.

Public Safety Answering Points (PSAPs) should be included. But even if the definition is limited to PSAP and 911 numbers (collectively, "Emergency Numbers"), the development and implementation of a list would be complex. As the Commission is aware, there is no master list of PSAP or 911 callback numbers. TelTech's experience working with the Commission and the National Emergency Number Association (NENA) in recent months confirms that even gathering the information on this narrow category of critical PSAP numbers is beyond the capability of a single carrier or trade association.

TelTech has been working with the Commission and NENA in an effort to help identify numbers for inclusion on a suitable critical call list to be permanently whitelisted. The genesis of the project was the realization that when a call to a 911 PSAP is unintentionally disconnected (for whatever reason), the emergency dispatcher will immediately place a call back to the caller ID of the dropped call. However, the recipient will not see "9-1-1" on their caller ID, but rather a number unknown to the recipient.

Absent a white list, call analytics services, like the callback recipients, cannot identify these numbers as emergency lines. This means that a carrier, app, or other service provider could unintentionally block a callback from a PSAP in an emergency situation. The Commission staff and TelTech realized that preventing accidental blocking of these and other emergency callback numbers should be prioritized.

Commission staff put TelTech in touch with NENA in an effort to identify a list of PSAP numbers. NENA explained that due to the independent nature of 911 centers, there is no centralized list of and emergency numbers currently available. It is likely there are more than 60,000 numbers that may potentially be used by PSAPs for outbound calls.

NENA and TelTech have worked together in recent months to identify and implement a solution. As a starting point, NENA is developing a voluntary program to try to get PSAPs to provide contact information through a yearly census. In addition, NENA is working on automated processes to collect and maintain this information. Because PSAP participation will be voluntary and subject to the decisions of administrators of the individual PSAPs that constitute this fragmented network, it is unlikely that this NENA system will ever achieve anything close to 100% capture of relevant emergency numbers.

Until this lack of a comprehensive list is rectified, the implementation of the proposed rules - or any rule that permits network-based blocking - presents a danger to public safety, as emergency numbers could accidentally be blocked.

Moreover, numerous commenters are pushing to expand a Critical Calls List to include the telephone numbers of a wide array of "entities forming the backbone of emergency services." This could include, among others, police departments, fire departments, health departments, hospitals, departments of emergency management, and similar agencies. Other commenters propose the inclusion of numbers used by entities that "broadcast" alerts about a wide variety of events, including school closings, severe weather, natural or man-made disasters, active shooter incidents, lock-downs, utility outages, product safety recall notices, and even such routine events as healthcare reminders, prescription notices, and mortgage servicing calls required by law.[24]

Both the Commission and numerous commenters have already identified the network security and robocall risks raised by having a centralized Critical Calls List. Those dangers are real and will be multiplied if the types and sheer quantity of telephone numbers on a Critical Calls

[24] *See, e.g.,* Comments of the Professional Association for Customer Engagement at 7; CUNA Comments at 6-8; INCOMPASS Comments at 10-11; and Comments of the Joint Trade Associations at 2-3.

List balloon. Balancing the need to ensure that all critical calls reach their destination and the need to ensure that bad actors are prevented from exploiting the Critical Calls List will be difficult.

Based on its experience, TelTech believes that the Commission (through its designated contractor, as with USAC) should create and maintain a Critical Calls List. Beyond the inclusion as many of the crucial PSAP/911 numbers discussed above as possible, TelTech is agnostic as to the scope of the list. However, as the scope of a Critical Calls List expands beyond Emergency Numbers, the potential security risks increase and the benefits become less obvious. TelTech believes that the Commission should weigh the costs and benefits of such expansion carefully.

The reality is that each voice service provider or analytics program developer (*e.g.*, First Orion or TelTech) will develop its own version of a Critical Calls List, regardless of whether there is a centralized list. Those lists will in each case include, but not be limited to, any centralized Critical Calls List. The benefit from the existence of a centralized list (whatever its scope) is that the compilation and ongoing list maintenance work need only be done once by a single entity, with the results made available to all authorized providers. The voice service providers and analytics program developers would not need to waste resources by duplicating each others' efforts.

TelTech agrees with those commenters who propose that if it implements an expanded and centralized list, the Commission should consider a middle ground approach that holistically identifies and permits critical calls. The Commission should not mandate that all numbers on an expanded Critical Calls List automatically be non-blockable. Given the inevitability that bad actors will spoof numbers on the list, the Commission should leave voice service providers the freedom to apply other analytics to determine whether a number on the list has been compromised and is being used to send robocalls. Service providers should be free to take into account other factors, including the SHAKEN/STIR attestation rating associated with the call (if any), calling

patterns, reports of emergency situations in the area where the called party is located, and other factors associated with the likelihood that the caller is or is not who they purport to be.[25]

Over time the analytics and the algorithms will improve and false positives leading to incorrect blocking will become rare occurrences.

B. Use of White Lists

In the *Declaratory Ruling*, the Commission authorized voice service providers to block unwanted calls using white list programs, which it identified as programs that block all calls from numbers not saved in an individual consumer's contact list.[26] The *Third FNPRM* seeks comment on other ways to block calls that would protect callers from erroneous blocking, and on any other bases for blocking unwanted calls.[27]

TelTech has been involved in developing white lists for its various consumer applications for more than half a decade. TelTech's consumer applications RoboKiller and TrapCall operate white lists that are specific to each individual customer. This is achieved by starting with the contact list on the customer's phone. This is precisely the type of simple white list contemplated by the *Declaratory Ruling*.

TelTech's white list program goes far beyond the approach approved by the Commission. TelTech long ago took advantage of the fact that "the evolution of technology has allowed the evolution of white-list programs."[28] As its mobile apps have always focused on protecting consumers' privacy and security on their mobile phones, building effective blacklists and white lists into our services has been a key area for TelTech. This is especially true for RoboKiller and

[25] *See* First Orion Comments at 11-12; USTelecom Comments at 3, 9-12; COMCAST Comments at 10-13; NCTA Comments at 10-12; TNS Comments at 10-12; Comments of CTIA-The Wireless Association at 21-22.
[26] *Third FNPRM* ¶ *43.*
[27] *Id.* ¶ *70.*
[28] *Id.* ¶ 43.

TrapCall. With these products, customers rely on TelTech to make effective call blocking decisions for them on incoming calls outside of their contact lists. In addition to ensuring that all contacts in a user's digital address book are automatically whitelisted, TelTech provides features on both RoboKiller and TrapCall to enable consumer level whitelisting of individual numbers. This allows a user to ensure that a number they input into our mobile app will never be blocked, even if they have not added it to their contacts list.

TelTech also long ago recognized that many calls that a customer would choose to receive if given the opportunity to make an informed choice come from numbers that are not in the customer's contact list and with which the customer has probably had no prior interaction. In other words, some fraction of calls from callers not known to the customer are "wanted" by the customer. Therefore, TelTech supplements the customer's own contacts list in two ways. The first is with its own version of the proposed Critical Calls list. Although as discussed above TelTech has been working diligently with NENA and other government agencies, they have to date only been able to identify and provide TelTech a small percentage of the universe of Emergency Numbers for inclusion on this permanent white list. Those Emergency Numbers that TelTech obtains and other numbers it concludes should never be blocked are permanently whitelisted and can only be removed from TelTech's white list manually.

TelTech also supplements its customers' individual white lists and the Emergency Numbers list with a more fluid proprietary list containing numbers that TelTech's algorithms have concluded - based on reporting by and the behavior of hundreds of thousands of TelTech customers - have a very high probability of originating calls that are "wanted."[29] For example, multiple users

[29] Nowhere in the *Declaratory Ruling* or *Third FNPRM* does the Commission define what specific call characteristics would warrant classification as an "unwanted" call. Such a determination is inherently subjective and logically can only be a consumer-specific determination. *See* West Telecom Comments at 8.

whitelisting the same number would be a strong indicator that a number should generally be whitelisted. TelTech adds or deletes numbers on this supplementary white list on a continuous basis based on its customers' real-time feedback.

TelTech does not block calls from numbers on its combined white list. If a Critical Calls List is developed, TelTech will add those numbers to the global white list that it maintains for all its customers. This will ensure that none of those numbers are blocked.

In addressing the development and use of sophisticated white lists, it is crucial to keep in mind that such lists, like everything else associated with the robocall problem, are fluid. White lists have to be constantly updated to reflect changes in individual customers' contacts lists and blocking preferences, and to incorporate real time feedback demonstrating changed customer group perceptions of the desirability of calls from certain numbers.

For example, a trusted company can place both wanted and unwanted calls from the same phone number. A bank's fraud department might use a particular number to notify customers of suspected instances of fraud, and then a week later the same number can be assigned internally to the bank department that makes cold calls to sell mortgages. Not surprisingly, the group feedback from TelTech customers in the second week could soon cause the algorithm to remove the number from the white list.

Based on its years of experience with customers' white list use and expectations, TelTech agrees with the Commission[30] and various commenters that any whitelist program must

- Be offered on an opt-in basis only;
- Ensure that consumers understand they are disclosing the numbers contained in their phone's contact list to their voice service provider; and
- Disclose to consumers the types of wanted calls likely to be blocked and the risks of blocking wanted calls.

[30] *Third FNPRM* ¶¶ *43-44.*

The type of white list program employed by TelTech is not appropriate for use by all voice service providers. For example, giving voice service providers the ability to block calls from numbers not in a user's contact list assumes access to that user's contact list. This is not an option with non-IP landline phones, as there is no stored contacts list to access. Even for customers using mobile phones or IP devices, there may be significant obstacles to voice service providers' implementation of a subjective white list. The *Third FNPRM* seems to assume that voice service providers have direct access to their customers' contact list, but such a relationship generally does not exist. The contact list (or address book) on a customer's IP device or mobile phone is a feature of the operating system of that phone or device and is not provided by or normally accessible by the voice service provider. A provider has no automatic access to the list, nor any mechanism for identifying what numbers are stored in a user's address book. In contrast, a mobile app such as RoboKiller can interact with the individual customer's phone's operating system to obtain permission to access the customer's address book. Because of this flexibility, many voice providers have developed mobile apps or partnered with mobile app services in order to obtain access to customer contact lists. But any such access - as with RoboKiller - depends on the individual customer granting approval.

These white list implementation problems may be exacerbated if providers are required to include sophisticated white list analytics at no charge as part of their blocking programs. It is not clear that voice service providers have the ability or the real incentive to develop and update effective, analytics-based white lists. There is a real danger that over-blocking of useful and wanted calls may result if providers misuse a simple white list and it becomes the default basis for a blacklist. Consumers will suffer if a provider implements a blocking program that automatically

blocks calls from numbers just because they are not on a white list (including a Critical Calls List).[31]

Conclusion

TelTech strongly supports the Commission's efforts to combat unlawful robocalls and to encourage implementation of SHAKEN/STIR. But the blocking and safe harbor proposals in the *Third FNPRM* do not strike the right balance. They fail to consider the inherent shortcomings of the SHAKEN/STIR framework or the substantial costs and societal harm from the millions of wrongly blocked that will inevitably result from use of this single narrow factor as a basis for network-wide blocking.

The Commission should focus on encouraging the implementation of blocking programs that are based on reasonable analytics and should consider implementing a safe harbor for such programs.

Respectfully submitted,

_____/s/_____

Mark C. Del Bianco

Counsel for TelTech Systems, Inc.

Law Office of Mark C. Del Bianco
3929 Washington St.
Kensington, MD 20895
Tel: 301-602-5892
mark@markdelbianco.com

Meir Cohen
Co-Founder and CEO
Ethan Garr
Senior Vice President for Strategic Growth
TelTech Systems, Inc.
101 South Broadway
South Amboy, NJ 08879

[31] The risk of over-blocking wanted calls can be minimized but not eliminated if a customer has made an informed choice to opt-in to a service, as is the case with the existing Custom Local Area Signaling Services (CLASS) feature of traditional wireline service and as the Commission contemplates in the *Declaratory Ruling* ¶¶ 41-44.