Before the

Federal Communications Commission

Washington, D.C. 20554

In the Matter of	)	
	)	
Targeting and Eliminating Unlawful Text Messages	)	CG Docket No. 21-402
	)	

COMMENTS OF THE MESSAGING MALWARE MOBILE ANTI-ABUSE WORKING GROUP (M^{3}AAWG) ON THE NOTICE OF PROPOSED RULEMAKING

I. Introduction

The Messaging Malware Mobile Anti-Abuse Working Group (M^{3}AAWG) is pleased to offer comments on the Notice of Proposed Rulemaking (NPRM), Federal Communications Commission (FCC) 22-72, CG Docket No. 21-402 concerning Targeting and Eliminating Unlawful Text Messages released on September 27, 2022.

M^{3}AAWG is a technology-neutral global industry association. As a working body, we focus on operational issues of internet abuse including technology, industry collaboration and public policy. With more than 200 members worldwide, we bring together stakeholders in the online community in a confidential, open forum, developing best practices and cooperative approaches for fighting online abuse.

The NPRM proposes to combat illegal text messaging with the same kind of regulatory action – originating network and phone number authentication technology – that is now used to defend against spoofed telephone calls. But the U.S. mobile text messaging and voice telephony ecosystems differ significantly. Chief among these differences is the degree to which spoofing in particular – that is, the use of fraudulent phone numbers to deliver unwanted messages – plagues the two ecosystems. *Although spoofing is a major issue in voice calling, it is nearly absent in U.S. text messaging.* Nearly all illegal and abusive text messages are originated using valid phone numbers by a sending or hosting party who has access to the corresponding sending

account. There is no need for mandating technologies to identify what is already generally known – the true service provider and customer phone number originating a text message – or to prohibit the sending from unauthorized or invalid numbers – a potential form of abuse that is already well controlled in the U.S. text-messaging ecosystem. M^{3}AAWG believes that identifying appropriate regulatory action requires a thorough understanding of the sources and types of illegal messages, as well as existing safeguards and practices which help mitigate illegal messages. In our comments we summarize these and offer specific comments on several of the questions posed in the NPRM.

II. Attack Methods and Sources

1. Most unwanted text messages originate from known sources.

Nearly all illegal, unwanted and abusive text messages originate from over-the-top service providers; emails sent to email-to-text gateways; or banks of illicit computer-driven mobile network devices, historically in this order of descending prevalence.

2. Accounts are owned by attackers.

In the vast majority of cases, the sender is using phone numbers that have been assigned to them, perhaps obtained anonymously and/or using deceptive information. Unauthorized account access is a problem, whether by unauthorized porting, password guessing, bribery, social engineering or other means. Here, industry standard best practices for account security have been established (but not always followed) especially by end users mismanaging their account credentials. That said, the greatest number of abusive messages originate from accounts assigned to, rather than hijacked by, the attacker.

3. Spoofing is rare.

M^{3}AAWG technical experts have no knowledge of even a single recent case in the US where an originating service provider has been able to transmit bulk messages to another service provider using numbers not registered to the originating service provider. STIR/SHAKEN, as widely implemented, seeks to prevent spoofed telephone calls and to hold senders accountable by identifying an originating (or, in some cases, transmitting) service provider and originating phone number – incorrectly referred to as “Caller ID Authentication” in the NPRM). Attacks that involve unauthorized use (such as porting fraud and account theft) are not prevented by

originating service provider and/or sending number identification – the information provided by the practical STIR/SHAKEN implementations. Any intra-service provider spoofing (e.g., "reflection spoofing," where a message appears to be sent by the recipient) is better addressed by the affected service provider correcting issues with its user authentication and/or identification mechanisms. (It should be noted that sending oneself a message is an allowed practice; some consumers do this to create reminders.) Therefore, in the U.S. text messaging ecosystem, there is essentially zero benefit from anti-spoofing implementations such as those of STIR/SHAKEN in U.S. voice telephony.

III. Existing Industry Defenses

4. Predetermined text message routing prevents spoofing.

Industry text messaging defenses include checks to help ensure that only legitimate and authorized users originate messages from their assigned numbers; systems for identifying and blocking unwanted messages; and various collaborative mechanisms for sharing information to empower the collective defenses of other organizations.

In the text messaging ecosystem, with only very rare exceptions, the originating service provider requires some form of user/account authentication such as a password, a token, or the authentication provided by a Subscriber Identity Module (SIM) inside a mobile device. The user or account is associated with one or more authorized phone numbers, and only messages from these phone numbers are accepted by the originating service provider. Further, in contrast to voice telephony practices, only the service provider to whom a given number is assigned is allowed to originate messages using this number. Messages may then be routed to other service providers for delivery, nearly always following a predetermined path determined by carriage contracts rather than dynamic routing algorithms used in voice. Central to this routing is the NetNumber ID (a service provider ID used in message routing) to which an originating phone number is assigned. At key points of aggregation along the transmission path, consistency checks are performed to ensure that the originating phone number is valid and assigned, and is consistent with the interface corresponding to the route along which messages from the originating service provider are expected to travel. In contrast to voice telephony, a receiving or intermediate service provider can therefore reliably determine the source of a message simply by performing a lookup of the originating telephone number in a routing registry (e.g., the Override

Services Registry or, for toll-free numbers, Texting & Smart Services [TSS] Registry). A message originated using service provider A's phone numbers will be blocked if received on an interface connected to service provider B. This system already prevents spoofing and the use of invalid phone numbers. It also provides information useful for real-time spam filtering and holds originators responsible for messages they send. This obviates the need for the hop-by-hop tracebacks necessary in voice telephony.

5. **Multiple points of intervention allow the industry to combat rogue content and senders.**

A key industry activity involves identifying message contents and senders of messages that recipients would find objectionable, and subsequently blocking them. An important mechanism for identifying unwanted messaging is end-user feedback – complaints from recipients (e.g., junk reports or spam reports). Over 11 years ago, industry implemented the 7726 (spells "SPAM") reporting system whereby users forward unwanted messages to short code 7726.

Since then, several device and mobile operating system manufacturers have improved end-user feedback by providing links and menu options within native text messaging apps. In the second half of 2022, these industry actions have increased the likelihood of an unwanted message being reported by over 25 times, while providing more accurate and more complete information (e.g., fewer erroneous spammers' phone numbers and more accurate timestamps). This advance is providing information that is resulting in faster and more accurate blocking, especially in the case of small or highly varying attack campaigns. Within M^3AAWG, network operators, handset manufacturers and security vendors work to continually improve this capability. Other unwanted message identification mechanisms include machine learning, sending patterns such as high message volume, detection of unexpectedly similar content from multiple sources and consideration of resource reputation (e.g., of domains, IP addresses and various types of service providers used in a message or its linked sites).

Industry defense mechanisms utilize properties of messaging identified as unwanted to select and enact enforcement actions. These processes are primarily implemented using extremely complex systems that rapidly adapt to constantly changing threats. Enforcement actions may be automated or manual and may include, but are not limited to:

- Blocking or throttling messages.

- Blocking senders, canceling accounts.
- Automated unwanted-traffic notifications sent to peer service providers.
- Feeds to anti-phishing and safe browsing organizations.
- Takedown requests to malicious sites' hosting providers and domain registrars. and to Government regulators and law enforcement in a manner consistent with privacy and compliance regulations and policies.

6. Collaboration and data sharing are key to defense.

Collaboration and data sharing are important aspects of defense against unwanted and illegal messaging for at least two reasons. First, additional layers of defense provide greater protection and complicate the efforts of attackers to circumvent them. Second, they allow for specialization in defense.

As an example, let us consider a hypothetical campaign of messages driving mobile subscribers to websites that phish for bank account credentials. An attacker might obtain an internet domain name similar to that of a large "example" bank (e.g., "example-security.com", similar to the hypothetical bank's "example.com" domain). They would then gain access to a server and use it to host a fraudulent look-alike bank website, using a commercial reverse proxy service to hide the IP address of that server. The attacker might also create an account with a text messaging service provider using a prepaid debit card and obtain one or more sending phone numbers. With these resources active, the attacker can conduct a text message campaign alerting victims to an issue with their bank accounts and direct them to the fraudulent website. Once bank and account numbers are obtained, they may be sold to a "carding" gang on anonymous internet chat sites using cryptocurrency. The gang would then create cards with the phished credentials and use them to get money from ATMs or purchase goods and services.

Such an attack might hypothetically be disrupted at any or all of the following points:

- Proactive domain discovery near the time of domain registration (the domain is lexically similar to the hypothetical bank's domain).
- Domain discovery by messaging spam filters.
- Discovery of sending number, domain and text pattern by spam filters.
- Discovery of sending number, domain and text pattern from end-user reports.
- Takedown requests and advice to the originating messaging service provider, domain registrar and reverse proxy operator.

- Identification of the real server hidden by a reverse proxy service.
- Discovery of potential victims based on collection of identified phishing messages recipients.
- Discovery of potential victims based on collection of copies of phished credentials.
- Notifying the bank of an active campaign and optionally providing them with information on attacks specifics and victim identity.
- Locking of victim bank accounts until new account credentials are established.
- Blocking of text messages based on identified malicious content.
- Blocking all messages from identified malicious senders.
- Takedown of attacker's messaging account.
- Blacklisting of identified domains in safe browsing domain blacklists to prevent potential victims from accessing the fraudulent website.
- Law enforcement and regulatory actions.

What is clear is that the collective defense against bad actors is empowered by the rapid collection and sharing of information. This might begin with an internet Domain Name Service (DNS) specialist discovering suspiciously named new domain name registrations made with a registrar having a history of being used to register phishing domains. (This identification might have been aided by having information on the actual party registering the domain name; however, this registrant information is generally no longer available even to DNS defense experts.) A bank, if provided with a list of victims, might lock accounts or add extra layers of security (e.g., block logins from new devices or unexpected geographic locations). The bank might then help the victims change their account credentials. While it might be possible to retrospectively identify recipients of phishing messages or visitors to a phishing site, privacy concerns may preclude potentially useful information (e.g., message recipient phone numbers) from being shared with the bank.

The power of collaboration is, to some extent, in conflict with the privacy rights of many parties. Even where laws permit sharing of information such as Customer Proprietary Network Information (CPNI) or Sensitive Customer Data (SCD), such information might not be shared so as to prevent occasional sharing of erroneously misclassified CPNI or SCD. More on this later.

Defense against unwanted text messaging is fueled by collection and dissemination of threat intelligence to other specialists in positions to use that information to disrupt attacks and direct defense actions towards abusive, negligent and complicit parties. This collaboration plays an important role, and is typically born of forums, including M^3AAWG, where experts converge to teach, learn and collaborate.

7. Know Your Customer.

All or nearly all Application-to-Person (A2P) sending service providers have the ability to identify, vet and mitigate abuse by their A2P messaging customers through a process known as Know Your Customer (KTC). KYC is a process that begins with verifying each customer's identity and risk profile, and continues with ensuring that terms and conditions of service are adhered to. Most service providers have compliance teams whose sole job is to act on indications (e.g., suspicious activity and/or complaints from others) of non-opted in, illegal and abusive text messages, and who can hold the senders accountable for violations of terms of service and acceptable use policies. M^3AAWG has maintained training and best common practices documents for its members to help create successful anti-abuse and compliance teams. These teams have been at the forefront of handling abuse issues for decades. In the text messaging space, most if not all reputable service providers maintain rigorous KYC practices, helping to ensure that only legitimate entities originate messages and minimize abusive messaging.

8. A2P registration has reduced spam and abuse.

The messaging industry, as it stands today, uses several registries already in place that map a sending number to the brand, content provider, and network originating the message. This accomplishes and often exceeds the goals of providing caller phone number and originating service provider information in the predominant STIR/SHAKEN implementations. This level of granularity has been implemented by members of the messaging ecosystem in a proactive effort to mitigate spam and abuse and improve the reliable delivery of wanted messages.

Self-regulated registries have contributed to a reduction in spam and an increase in accountability. It should also be noted that accountability for messages identified as malicious or unwanted results in the creation of accurate markers for reputation and trust of brands and content service providers. These markers increase the accuracy of systems and processes that

throttle or block messages deemed to be untrustworthy based on abuse complaints and other factors.

9. Consumer education increases reporting of abuse.

Industry and Government both participate in educating consumers on what to do and what not to do when they receive suspicious or malicious messages. An educated consumer is a safer consumer. Consumers that are educated to report abuse help make other consumers safer.

10. Existing defenses are strong.

Working in a complementary way, sender authentication, anti-spoofing mechanisms, spam blocking systems, education, data exchange and collaboration within industry as well as with Government help make text messaging one of the safest of open and interoperable electronic communications media. The U.S. text messaging industry's defenses are strong. Voice and text ecosystems (including aspects of technology, abuse, existing defense mechanisms and regulation) are not the same. What may have been needed for voice has similarities, but much of the action taken to mitigate voice abuse (e.g., anti-spoofing, blocking of unassigned numbers) has long been standard industry practice in inter-carrier text messaging. Lighter regulation of text messaging has helped service providers and the ecosystem all of whom vye for customers in a highly competitive market – take steps to mitigate abuse that threatens and annoys customers and harms one of the most important communications media of an open society.

IV. General Comments

11. New regulations become outdated and can compound the problem they were meant to solve.

Abuse is unfortunately enabled by open and readily available communications media. Industry and Government strive to maximize accessibility and reliable delivery of appropriate communications while blocking unwanted and/or illegal communications. Rapidly advancing technology creates an arms race between abusers and defenders. New technologies can evolve and spread instantly by way of cloud-based apps and social networks and may take hold with little oversight. At times, even industry struggles to erect new defenses. In some cases, prior regulations (e.g., certain Title II call completion and "you may use your number to call from any CLEC" regulations) deemed beneficial at the times of promulgation may now actually inhibit or

prevent beneficial industry actions when advancing technology brings new forms of abuse. We observe that the less-regulated text messaging industry has had anti-spoofing technologies in place for well over a decade and is now advancing beyond service provider registration with registration of high-volume A2P senders (e.g., brands) themselves. We urge the FCC to consider the risks of creating regulation in spaces where industry already has solutions in place. While M^{3}AAWG acknowledges and appreciates the FCC's activities and efforts to make text messaging safer, we believe that the messaging industry is more likely to rapidly mitigate new levels and vectors of abuse that are found daily without regulations that may lag industry action and potentially encumber the mitigation of future issues. In text messaging, regulatory policy changes that may have been needed in the telephony ecosystem to relax Title II service regulations (e.g., to facilitate robocall blocking) are unneeded. The light touch of Government regulation of text messaging has facilitated industry's creation of bodies that enable self-governance. This absence of excessive mandates has enabled the industry's successes, most notably making text message spoofing so rare.

M^{3}AAWG's technical subject matter experts have found that the fight against abuse is significantly improved by the sharing of threat information, regular training, and adherence to the recommendations of best common practice documents. This also includes educating consumers to avoid falling victim and to report abusive messages, and continues with threat information sharing between service providers and the larger cybersecurity community. The FCC has played a key role in many of these areas, taking a leading role in consumer education, helping to open data-sharing channels by clarifying and raising awareness of security exceptions in regulations needed to protect parties' private information, and providing safe harbor for occasional missteps where appropriate.

M^{3}AAWG encourages the FCC to continue its efforts to educate consumers about the risks presented by illegal messages and the best ways to handle unwanted and illegal messages.

We also encourage the FCC to promote appropriate sharing of data between organizations that may help mitigate abuse, including raising industry awareness of various exceptions to privacy regulations where certain actions might mitigate abuse and, where reasonable, crafting safe harbors and permissive regulations to encourage responsible sharing of abuse data.

For their part, to better protect consumers, U.S. mobile operators are now implementing bulk messaging campaign registration processes and systems that increase oversight of automated bulk messaging and help hold rogue senders accountable. Service providers are now required to submit brand and messaging campaign information for vetting and approval prior to sending. This registration process helps to ensure that the brand understands the CTIA recommendations as well as individual carriers' requirements for non-consumer message senders. As all phone numbers used in a messaging campaign must be declared, this helps defeat "snowshoeing" (i.e., the use of up to thousands of phone numbers in a single messaging campaign to circumvent spam filters) and allows enforcement actions at a brand and messaging campaign level. It also helps ensure reliable delivery of wanted messages.

V. Comments on Specific NPRM Questions

In this section we offer comments on specific questions asked by the Commission in the NPRM.

III. DISCUSSION

A. Mandatory Blocking of Illegal Texts

19. Mandatory Blocking of Texts Purporting to be From Invalid, Unallocated, or Unused Numbers or on the Do-Not-Originate List.

As discussed above, intercarrier text messages from invalid, unassigned and unallocated NANP numbers are already generally blocked by existing anti-spoofing checks.

A 2022 M^{3}AAWG member study found that out of approximately 13 million messages for which consumer complaints were received, 325 originated from numbers found in the voice DNO list. Some were unwanted, but none appeared to be illegal or showed signs of being spoofed. This illustrates that there is little benefit to using the existing DNO list to mitigate illegal text messages. The survey did not produce information on how many legal messages from DNO numbers might have been mistakenly blocked. However, M^{3}AAWG experts believe that even a text-specific DNO list would, given its purpose of blocking certain spoofed messages, do more harm than good in the text messaging ecosystem where spoofing is rare.

20. Additional Measures to Prevent Illegal Texts from Reaching Consumers.

Spoofing is not a significant issue in text messaging, so additional service provider identification technologies such as those of STIR/SHAKEN are unnecessary. More precisely, in

the text messaging ecosystem, with only very rare exceptions, the originating service provider is easily identified by a simple lookup without the need for a hop-by-hop traceback. In voice the rightful owner of a telephone number may originate calls from essentially any service provider of their choosing, and individual calls may flow through dynamically-selected paths to the terminating service provider. With text messages, only the service provider of record is authorized to originate text messages using numbers registered to themselves, and messages generally follow a shorter, deterministic path from originating to terminating service provider. The hop-by-hop practices of first comparing the interface on which a message was received to the interface that would be expected given the originating phone number, and then blocking messages where inconsistency is detected, effectively block spoofed messages. They have the beneficial side effect of also blocking invalid, unallocated and unassigned numbers. As mentioned before, M^{3}AAWG technical experts have no knowledge of even a single recent case in the U.S. where an originating service provider has been able to transmit bulk messages to other service providers using numbers not registered to the originating service provider.

STIR/SHAKEN as widely implemented in the voice telephony ecosystem seeks to prevent spoofing and hold senders accountable by identifying an originating (or in some cases gatewaying) service provider. But attacks that involve unauthorized use such as porting fraud and account theft are not prevented by originating service provider identification, such as that of practical STIR/SHAKEN implementations. Any intra-service provider spoofing (e.g., "reflection spoofing," where a message appears to be sent by the recipient) is best addressed by the affected service provider correcting flaws in its user authentication. This means that there is essentially zero benefit from anti-spoofing implementations such as those of STIR/SHAKEN in voice telephony.

21, 22 and 23. Need for Mandatory Blocking.

As discussed above with respect to NPRM sections 19 and 20, "voluntary" blocking is already practiced by all major US carriers and inter-carrier vendors. There would be no perceptible benefit from mandating such regulation. And, as discussed earlier, any regulations created now might cause unanticipated issues in the future.

Most unwanted message campaigns use changing phone numbers, changing internet domains and/or varied text. And even if they do not, a community benefits from an analysis of

traffic affecting the wider community, for which network-based blocking technology is most appropriate. In either case, effective blocking of bulk messaging is aided by a network view of current and past spam campaigns.

Over-the-Top (OTT) services may mean different things; a messaging service or application (e.g., WhatsApp) that is operated by a single company, or mobile text messaging (e.g., SMS or MMS) to or from a service provider that does not operate a mobile telephony network. This fact favors network-based approaches to message filtering. Some functions, such as blocking repeated messages from a single phone number (e.g., related to a failed relationship, or intended for another party) may be effectively handled by personal block lists. Unwanted, potentially subscribed message streams from a single phone number may be addressed by replying "STOP" or by personal blocklists. Personal blocklists may be network and/or device functions. *Overall, network-based blocking is capable of and responsible for blocking far more unwanted messages than device-based blocking.* It should be noted that some device-based spam filter implementations may query a network for information used to block; for the purposes of this discussion, these are considered network-based blocking. Blocking technologies benefit from a network-wide view of unwanted messages, and uniform network-based blocking simplifies remediation of mistaken blocking.

24. Standards to Ensure Competitively- and Content-Neutral Grounds for Blocking.

Unfortunately, certain negligent and/or complicit service providers have sent almost entirely (e.g., > 99%) unwanted text messages. Current blocking practices based on the originating service provider's behavior contribute greatly to the protection of end users. Modern spam filters are heavily dependent on the reputation of attack-related resources, including internet domains, IP addresses, hosting providers, domain registrars, service providers and many others. We have observed that the FCC has also found it necessary to take actions against specific service providers. Blocking technologies based solely on the sending history of an individual phone number or specific content cannot provide an adequate defense against the most common attacks, which use constantly changing text, disposable phone numbers and internet links. Additionally, scoping specific blocking rules to specific service providers known to be sources of an attack prevents accidental blocking of wanted messages from other service providers. Any regulation preventing a service provider from holding other service providers

accountable for the traffic they originate degrades defenses and disincents service providers from managing abuse originating in their network. Regulations intended to prevent anti-competitive practices can and will degrade consumer protection by preventing rogue service providers being held accountable for their misbehavior.

25 and 26. Emergency Texts.

Any regulation that seeks to prevent the erroneous blocking of emergency texts should include provisions for operators and senders to protect the emergency services *themselves* from threats. Considerations should allow for implementation of protections to include (but not limited to) denial-of-service blocking defenses (e.g., hailstorm and/or snowshoe attacks) as necessary, and also anticipate occasional mistaken blocking incidents.

The Internet Crime Complaint Center (IC3) in January 2013 and the FBI in February in 2021 have issued warnings concerning telephony denial-of-service attacks against several 911 call centers. Even if history were to tell us that blocking 911 messages has never been advised, such a time may come, and it is important to allow agile spam defenses to be rapidly employed when needed to protect critical services. As Next Generation 911 systems (NG911) become more available in regions, it becomes increasingly likely that a malicious actor may initiate a regional attack such as a botnet-enabled denial-of-service attack. As technology advances and text-to-911 gains popularity, text messaging attacks on Emergency Services become more likely. Regulations preventing any blocking of Emergency Services could create an undesired or even dangerous result. We see every reason to believe that voluntary processes and procedures established by Emergency Services and carriers are more likely to have the needed ability to adapt to technology advances.

27. Mitigating Erroneous Blocking.

Service providers cannot in general be expected to determine the legality of a given message. With very limited exceptions, where legality may intersect with technical aspects such as spoofing, service providers cannot be expected to enforce blocking based on legality, either. Blocking is guided by service providers' terms of service, which are in turn guided by industry standards. Examples are opt-in/opt-out mechanisms and notices and consent requirements. As in email, blocking decisions are impacted by indications of consent to receive, malicious intent,

and recipient annoyance. That said, the result is that a large fraction of illegal messages are blocked. In U.S. text messaging, consumer complaints are a major if not the primary input to blocking decisions. Any shift towards basing delivery decisions solely on legality determinations would result in a dramatic increase of abusive, illegal and unwanted messages received by consumers.

Given that many millions of messages are blocked daily – using a combination of millions of message "fingerprints," message blocking rules, sender/receiver reputation and consumer feedback, and by many layers of defense (e.g., of device and network vendors' blocking systems) – it is difficult to envision a set of regulations governing general text-message unblocking processes and procedures that would be workable and cost-effective. Existing processes and procedures based chiefly on contractual relationships are generally effective in these cases.

III. DISCUSSION

B. Applying Caller ID Authentication Requirements to Text Messages

28. Implementing Caller ID Authentication.

The Commission should be aware, as stated above, that nearly all unwanted and abusive U.S. text messages originate from parties that have control of the service provider account to which the originating phone number is assigned, and use that service provider account to originate abusive messages. This is because the problems that technologies such as STIR/SHAKEN seek to solve in the voice telephony ecosystem have already been solved in U.S. text messaging. Current industry agreements and practices provide reliable identification of the originating service provider and phone number. Hop-by-hop consistency checks have a proven record of preventing service providers from transmitting messages to other service providers using numbers not assigned to them. Specifically, in contrast to voice telephony, interservice-provider text message routing is deterministic. Messages purporting to originate from one service provider are only expected on certain interfaces. If anomalous, they are blocked. While STIR/SHAKEN and similar mechanisms can help mitigate unauthorized message origination and in-flight envelope alteration (e.g., changing the calling number), the text messaging ecosystem's existing security practices and procedures are already highly effective. Spoofed-number security incidents have been reported (e.g., "sent from my own number" spam campaigns as reported in

the press). However, a STIR/SHAKEN-like mechanism, generally applied after a service provider's rarely-defeated internal originating number authentication, would be no more effective in empowering blocking than existing anti-spoofing mechanisms. We are not aware of any rational basis for expecting that the application of STIR/SHAKEN or similar technology to U.S. text messaging would result in a perceptible reduction in unwanted or abusive text messages. Like the voice experience in jurisdictions where service providers are only allowed to originate communications from numbers assigned to them, spoofing is not a significant problem in text messaging. Requiring additional mechanisms to "solve" it would result in misallocation of resources that would better be applied to other anti-spam mechanisms. It would also likely increase erroneous blocking attributable to operational errors in the application of more complex authentication mechanisms. In summary, mandating the application of STIR/SHAKEN or similar mechanisms to the existing U.S. text messaging ecosystem would be expected to moderately degrade rather than improve the consumer experience.

Therefore, no practical originating or gatewaying service provider authentication mechanism (such as the typical U.S. voice STIR/SHAKEN implementation) that helps to identify the originating service provider will be of significant benefit. Further, there are no indications that existing mechanisms for identifying the originating service provider are likely to fail in the foreseeable future.

30. Ability of current STIR/SHAKEN governance system to accommodate authentication.

Existing STIR/SHAKEN technology and the current governance for U.S.-based voice implementations are of limited applicability to and/or are inappropriate for text messaging. Many text message content service providers do not have the registrations required by the STIR/SHAKEN governance model. These registrations constitute a significant burden, especially to smaller providers. Lightly-regulated text messaging service providers could be forced to obtain an Operating Company Number (OCN), complete 499A filings as a Universal Service Administrative Company (USAC) contributor, apply to become a Numbering Authority, complete STI Policy Administrator (STI-PA) test planning, procure a certificate and engineer a solution that would insert that certificate into the call flow.

Certificate rotation and management also present non-trivial operational challenges which would be exacerbated by a mandate to use a telephony-specific issuance authority rather

than self-issued credentials or certificates issued by any well-known and trusted certificate authority.

Alternatively, voice providers can pay for an API-based product offered by certain Certificate Authorities that will sign calls – thus possibly losing their more-granular unique identity and assuming an identity shared with other providers. Either path poses significant financial, technical, and administrative burdens, particularly for smaller providers, and are unnecessary in the text messaging ecosystem where number spoofing is extremely rare.

In the lightly regulated text messaging ecosystem, individual service providers are able to rapidly hold each other accountable for illegal and non-compliant messaging. This distributed model allows for faster and more effective action than a centralized or industry-consensus-driven model could.

Therefore, we recommend that the Commission adopt no regulations requiring STIR/SHAKEN service provider governance to be applied to text message service providers.

III. DISCUSSION

C. Other Actions

37 and 38. Increased and Updated Consumer Education.

The FCC's Consumer Tips and other consumer education efforts are an important component of a comprehensive abuse mitigation strategy. However, many consumers have been conditioned and/or educated NOT to respond to any messages received from unknown or unrecognized sources, even when the sender provides opt-out options (e.g., "Stop2End"). Although opt-out responses can be used in harmful ways, serious consequences (that is, consequences beyond what might result from the recipient knowing that a live human received the message) are exceedingly rare. Most messages that present an opt-out option are from legitimate senders. "STOP" responses are likely to prevent additional unwanted messages from being received and are typically observed by defense systems which sense excessive "STOP" responses and help take action against unconsented message senders. M^3AAWG recommends educating consumers that they may choose to reply "STOP" after receiving multiple unwanted messages from a sender.

Additionally, spam reporting functions built into mobile devices are now the preferred method of reporting unwanted or illegal messages. However, these are not available on all

devices or in all situations. We recommend that consumers be encouraged to report using built-in reporting functions where possible, and where not possible, to forward messages to Short Code 7726.

We suggest that the FCC's Consumer Tips, such as those in the press release accompanying the subject NPRM, be updated for consistency with M^3AAWG and other text spam reporting best practices as follows. (Suggested tip updates are highlighted):

Consumer Tips:

- If you receive multiple spam messages from a sender, reply "STOP" to request removal from their mailing list. Otherwise, do not respond.
- Do not click on any links.
- Do not provide any personal information via text or website.
- File a complaint.
- Use your phone's text messaging spam reporting features, if available. Otherwise forward unwanted texts to SPAM (7726).
- Delete all suspicious texts.
- Update your smart device OS and security apps.
- Consider installing anti-malware software.
- Review companies' policies regarding opting *into and* out of text alerts and selling/sharing your information before consenting to receive texts.
- Review text blocking tools in your mobile phone settings, available third-party apps, and your mobile phone carrier's offerings.

Industry and Government Can Work Together Towards Voluntary Actions

Given the need for greater public protection from text messaging threats and the risks of regulation unintentionally encumbering industry defense efforts, we urge the commission to work with industry to voluntarily adopt commitments that move towards the shared goal of mitigating unwanted and/or illegal text messaging. Potential areas of commitment include continued study and/or development of appropriate authentication technologies and adoption of a reasonable and practical set of best practices. Best practices might include commitments to, as technology advances, maintain existing defenses and, where practical, deploy new defenses

against messages originating from spoofed, invalid, unallocated and unassigned North American Numbering Plan phone numbers.

VI. Barriers to Information Sharing

New privacy regulations have caused previously available information to be withheld from law enforcement and industry cyberdefense experts, exposing consumers to increased threats of malicious messaging and other cyberthreats. Nowhere is this more evident than in the restriction of information on many internet domain registrants. Here privacy regulations – including but not limited to Europe's General Data Protection Regulation (GDPR) – have resulted in the barring of the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Assigned Numbers Authority (IANA), and registrars from freely providing information such as identification of a party that has registered or operates a malicious website to qualified security practitioners or researchers. WHOIS records are an essential resource used by cybersecurity experts, law enforcement agents, blocklist providers and others to attribute criminal activity, understand malware campaigns, flag malicious domains, and more.

The public has an interest in privacy as well as in security. In some cases, these are currently out of balance, as the needs of security practitioners and law enforcement are at times addressed without consideration of privacy. Privacy regulations, without appropriate exceptions to facilitate protection of the public, obstruct the work of security practitioners at significant cost to the public. The ultimate issues to be determined are the scope of the information that should be available to security practitioners such as M^{3}AAWG members; the availability of safe harbors to protect well-intentioned practitioners from occasional errors; and the proper role of the regulator. We urge the commission to ensure that any new regulations include both exceptions and safe harbors for the sharing of information that is vital to defense.

VII. Conclusion

M^{3}AAWG urges the FCC to consider that mandating a solution similar to STIR/SHAKEN in the text messaging ecosystem will result in no perceptible consumer benefit, and will divert resources from industry's ongoing efforts to improve text messaging safety through technical and other means. As outlined in the comments above, regulation will not help the messaging industry most effectively protect consumers from illegal and unwanted text messaging, and additional mandates might encumber or prevent implementation of needed

industry defense processes and mechanisms. With messaging technology rapidly advancing and abuse tactics morphing on what is sometimes a minute-by-minute basis, the messaging industry needs defense agility to match that of the attackers'. It is critical that each defender of the messaging ecosystem be afforded flexibility to ensure that text messaging remains a trusted and reliable medium of communication.

We see every reason to believe that the U.S. text messaging industry will take whatever steps are necessary to continue its nearly 100% success rate in preventing spoofing through its voluntary identification, development and adoption of appropriate best practices, terms of service and technologies.

Industry has recently been successful in dramatically increasing the accuracy and ease of consumers' unwanted message reporting and the volume of reports sent to carriers. This information enables carriers' defense systems to act more rapidly and precisely; defenses are becoming stronger. We encourage the FCC to help raise consumer awareness of the importance of reporting illegal and unwanted messages.

Sharing this ever-increasing body of threat information more widely can make text messaging and the entire online ecosystem safer as it empowers collaborative defense action. But this can happen only with regulations that properly balance privacy, privacy exceptions and safe harbor.

We encourage the Commission to rely on, promote and facilitate voluntary industry and consumer action through education; regulations that permit and even empower collaboration wherever possible; and any actions that can foster increased collaboration.

Thank you for the opportunity to submit these comments. We will be glad to respond to any questions. Please address any inquiries about our comments or work to M^3AAWG's Executive Director, Amy Cadagin.

Sincerely,

Amy Cadagin
Executive Director, Messaging Malware Mobile Anti-Abuse Working Group
P.O. Box 9125
Brea, CA 92822
amy@m3aawg.org