Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Targeting and Eliminating Unlawful Text Messages	)	CG Docket No. 21-402
	)	
	)	
Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991	)	CG Docket No. 02-278
	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	

REPLY COMMENTS OF CTIA

Thomas C. Power
Senior Vice President and General Counsel

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

Sarah Leggin
Assistant Vice President, Regulatory Affairs

Mike Beirne
Director, Regulatory Affairs

CTIA
1400 Sixteenth Street, N.W.
Suite 600
Washington, D.C. 20036
(202) 736-3200

March 11, 2024

TABLE OF CONTENTS

I. INTRODUCTION & SUMMARY. 1

II. THE RECORD CONFIRMS THAT THE WIRELESS MESSAGING INDUSTRY'S MULTI-LAYERED DEFENSES ARE PROTECTING CONSUMERS FROM BILLIONS OF UNWANTED AND ILLEGAL TEXT MESSAGES. 4

III. THE RECORD MAKES CLEAR THAT COMMISSION-IMPOSED BLOCKING STANDARDS WOULD UPEND TODAY'S BEST PRACTICES AND UNLEASH A FLOOD OF SPAM AND SCAM TEXT MESSAGES ON CONSUMERS. 6

IV. THE RECORD CONTINUES TO DEMONSTRATE THAT EFFECTIVELY MITIGATING SPAM AND SCAM TEXT MESSAGES REQUIRES A FRAMEWORK UNIQUE TO THE TEXT MESSAGING ECOSYSTEM. 10

A. The Commission Should Focus on Stopping Bad Actor Message Senders. 10

B. No Further Commission Action Is Needed on Text Authentication Solutions. 11

C. The Commission Should Avoid Stranding Legitimate Users of Email-to-Text. 12

D. CTIA's Secure Messaging Initiative is Ready as a Resource for "Traceback." 12

V. CONCLUSION. 13

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Targeting and Eliminating Unlawful Text Messages	)	CG Docket No. 21-402
	)	
Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991	)	CG Docket No. 02-278
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59

REPLY COMMENTS OF CTIA

CTIA respectfully submits these reply comments in response to the Federal Communications Commission's ("Commission" or "FCC") Second Further Notice of Proposed Rulemaking ("*Second FNPRM*") in the above-referenced proceedings seeking to protect consumers from illegal and unwanted text messages.[1]

I. INTRODUCTION & SUMMARY.

The record developed in response to the *Second FNPRM* continues to demonstrate that the messaging ecosystem's multi-layered policies, processes, and tools are having a significant impact in the fight against spam and scam messages.[2] As CTIA noted in initial comments, in 2023 alone, wireless providers *blocked over 47.5 billion spam messages* from reaching consumers. The result is a dramatically improving consumer experience, as shown by a near

[1] *Targeting and Eliminating Unlawful Text Messages et al.*, Second Report and Order, Second Further Notice of Proposed Rulemaking in CG Docket Nos. 02-278 and 21-402, and Waiver Order in CG Docket No. 17-59, FCC 23-107 (rel. Dec. 18, 2023) ("*Second Report and Order*" and "*Second FNPRM*").

[2] Comments of Verizon at 1, 4 ("Verizon Comments"); Comments of Twilio at 2–5 ("Twilio Comments'); Comments of CTIA at 5–9 ("CTIA Comments"). Unless otherwise indicated, comments referenced herein were filed in response to the *Second FNPRM* in CG Docket No. 21-402 on or about February 26, 2024.

40% drop in consumer complaints to the Commission and the Federal Trade Commission ("FTC") about text messages between 2021 and 2023.

As a coalition of six national consumer advocate organizations ("Consumer Advocates") recently observed:

> [T]exting currently remains a valuable and trusted method of communication in the United States, largely because of the best practices developed by CTIA and adopted by its members and their partners. . . . [T]he entire texting ecosystem would be a disaster if fewer industry-developed restrictions against unwanted texts were applied.[3]

The Commission itself also recently recognized these industry best practices and policies have "gone a long way to protect consumers" from spam and scam text messages.[4] While keenly focused on protecting consumers, wireless providers and their messaging ecosystem partners are committed to striking the right balance between that and facilitating legitimate message senders' use of text messaging to reach consumers.

The Commission should reject some commenters' calls to upend policies and practices that would expose consumers to the flood of harmful and unwanted text messages that the wireless messaging ecosystem is currently keeping at bay. Specifically, advocates for non-consumer message senders, like the VON Coalition ("VON"), INCOMPAS, and REACH, would have the Commission eliminate industry policies and blocking frameworks that are currently stopping the messages that consumers do not want to receive. Following the calls of those commenters would effectively guarantee that consumers receive text messages related to illegal substances, sex, hate, alcohol, firearms, and tobacco, or other high-risk messaging to

[3] Letter from Margot Saunders, Senior Counsel, National Consumer Law Center, to Marlene Dortch, Secretary, FCC, CG Docket No. 21-402 et al., at 2 (filed Mar. 6, 2024) ("Consumer Advocates Ex Parte").

[4] *Second Report and Order* ¶ 15.

which they have not consented. Non-consumer message senders that are pushing to send such content are akin to the illegal robocallers that the Commission is fighting hard to stop. The ensuing collapse in consumer trust would be the inevitable result of their calls to eliminate consumer safeguards, and the Commission should reject them.

The record also cautions the Commission against adopting other proposals in the *Second FNRPM* that are borrowed from the robocall playbook but are not tailored to address issues unique to the messaging ecosystem:

- First, the proposal to require originating providers to block certain telephone numbers would not be effective at blocking bad actor traffic because an originating provider is not the "choke point" for all illegal messaging traffic generated by a message sender. At the same time, doing so would pose a significant risk of blocking legitimate messages. The Commission should instead focus on identifying and stopping the message *senders* behind spam and scam texts.
- Second, the record continues to show that regulatory obligations to incorporate text message authentication solutions are unnecessary to address the main problem in text messaging: identity spoofing/impersonation. No further Commission action on text message authentication is needed or would be effective.
- Third, the Commission should encourage legitimate users of email-to-text messaging services—which include many government and public safety agencies—to migrate to more secure non-consumer messaging channels, rather than abruptly cut off these users from sending critical messages by adopting a consumer opt-in requirement.

- Finally, the record confirms that CTIA's Secure Messaging Initiative ("SMI") can and should serve as the Commission's resource for collaborative efforts and information sharing about suspected bad actors behind spam and scam texts.

The record shows that the messaging ecosystem is preventing tens of billions of unwanted and illegal text messages from reaching consumers each year, and the wireless industry and their messaging partners remain committed to continuing to develop new and increasingly sophisticated capabilities to match bad actors' evolving tactics and block messages that consumers do not want.

II. THE RECORD CONFIRMS THAT THE WIRELESS MESSAGING INDUSTRY'S MULTI-LAYERED DEFENSES ARE PROTECTING CONSUMERS FROM BILLIONS OF UNWANTED AND ILLEGAL TEXT MESSAGES.

Consistent with the record developed in this proceeding since 2022, the initial comments continue to demonstrate that wireless providers and their messaging ecosystem partners are investing enormous resources into systems and practices to combat spam and scam text messages and that those efforts result in considerable protection for consumers.[5]

For example, Verizon, like other wireless providers, "is fighting back hard with a comprehensive array of tools and strategies to prevent illegal and unwanted texts from reaching and otherwise impacting [its] consumers, and [it is] succeeding."[6] Among other messaging providers, Twilio noted that "all U.S. originating traffic on [its] network is registered and verified," and it has "dedicated significant resources to building a large team that verifies sender and service information" and "enhance[d its] fraud and mitigation capabilities."[7]

[5] Verizon Comments at 1, 4; CTIA Comments at 5–9; Twilio Comments at 2–5.

[6] Verizon Comments at 1.

[7] Twilio Comments at 2–3.

These efforts are having a tremendous impact in the fight against spam and scam messages.[8] In 2023, wireless providers blocked over *47.5 billion spam messages* from reaching consumers.[9] Verizon, for example, blocks more than one billion unwanted or illegal text messages every month.[10] And Twilio has developed a solution to prevent compromised accounts from sending messages on its platform that has resulted in a 300% increase in detection of these accounts.[11] Consumer response to these efforts is tangible and positive. In 2023, consumer complaints regarding text messaging *dropped nearly 40%* at both the Commission and the FTC as compared to 2021.[12]

The record also demonstrates that consumers are exposed to spam and scams throughout the broader messaging ecosystem, including on over-the-top ("OTT") applications, and not just through SMS/MMS.[13] As the Commission is aware, OTT messages are outside the SMS/MMS

[8] There is some data from YouMail in the record. The Commission should be cautious against drawing conclusions from this data. For example, it is possible that some of the data demonstrate how bad actors use account takeovers to send spam or scam text messages for a limited period of time, rather than demonstrating an intent by the providers or senders to send spam or scam text messages. *See* Comments of National Consumer Law Center et al. at 5 ("NCLC Comments"). As Twilio notes, messaging stakeholders continue to enhance their defenses against account takeovers. Twilio Comments at 4–5. And CTIA's SMI is a resource for helping to identify providers that may be facilitating unwanted and illegal text messages and helping industry and enforcement authorities partner to stop those unwanted texts at the source. These tools and frameworks will better protect consumers from unwanted texts than proposals to block all traffic from a given provider, which would risk blocking legitimate traffic while failing to stop all bad actor traffic.

[9] CTIA Comments at 5.

[10] Verizon Comments at 1 n.2.

[11] Twilio Comments at 4–5.

[12] CTIA Comments at 8. NCLC notes that while the number of complaints decreased in 2023, total financial losses increased. NCLC Comments at 3. This inverse relationship supports the call by CTIA, Verizon, Twilio, and others for more aggressive enforcement actions aimed at the senders of scam text messages. CTIA Comments at 13; Twilio Comments at 6–7; Comments of Verizon, CG Docket No. 21-402, at 10 (filed Nov. 10, 2022) ("The Commission has opportunities to partner with industry and with other agencies on aggressive enforcement aimed at deterring illegal text spammers and companies who support them."); Reply Comments of CTIA, CG Docket No. 21-402, at 15 (filed June 6, 2023); Comments of T-Mobile USA, Inc., CG Docket No. 21-402, at 3, 10–11 (filed Nov. 10, 2022).

[13] Comments of REACH at 5 ("REACH Comments"); NCLC Comments at 10; CTIA Comments at 9–10.

framework, "invisible to the consumers' providers," and are thus beyond providers' effective actions to maintain trust in text messaging.[14] OTT providers and other stakeholders have a role to play in protecting consumers, and a regulatory approach that continues to focus solely on SMS/MMS will not produce the results the Commission seeks in this proceeding.[15]

III. THE RECORD MAKES CLEAR THAT COMMISSION-IMPOSED BLOCKING STANDARDS WOULD UPEND TODAY'S BEST PRACTICES AND UNLEASH A FLOOD OF SPAM AND SCAM TEXT MESSAGES ON CONSUMERS.

The record continues to demonstrate that the wireless industry is committed to striking the right balance between protecting consumers from spam and scam text messages while facilitating legitimate message senders' use of text messaging to reach consumers. The Commission should reject calls by advocates for non-consumer message senders, like VON, INCOMPAS, and REACH, that would have the Commission eliminate industry policies that are blocking the messages consumers do not want in favor of a Commission-adopted standard that *would unleash a flood of unwanted text messages on consumers*.[16]

The Consumer Advocates lay bare the intent behind these efforts: "[t]he goal of all of their arguments is to allow their text messaging practices to be unconstrained by the current protections imposed by CTIA, the wireless providers and other partners."[17] The Consumer Advocates point out that one commenter "represents the telemarketers and lead generators responsible for flooding the nation's telephones with unwanted telemarketing calls and texts."[18] And they conclude:

---

[14] NCLC Comments at 10.

[15] CTIA Comments at 9.

[16] *See* Comments of Voice on the Net (VON) Coalition at 6–8 ("VON Comments"); Comments of INCOMPAS at 7–10 ("INCOMPAS Comments"); REACH Comments at 2–5, 7–8.

[17] Consumer Advocates Ex Parte at 2.

[18] *Id.* (citing REACH Comments).

> If the Commission were to bend to the wishes of these commenters and constrain the current protective measures, text communications would unquestionably follow the sad path of voice calls—people would no longer trust the mechanism and would no longer open and communicate by texts nearly as frequently as they do now.[19]

Today, messaging stakeholders protect consumers from billions of unwanted and illegal text messages by implementing vetting and registration policies and blocking frameworks informed by industry best practices.[20] These best practices include guidance on types of messages consumers do not want to receive and encourage adoption of unwanted messaging traffic policies that protect consumers in a manner that facilitates the exchange of wanted wireless messaging traffic.[21] The best practices also explain that providers may block or filter message traffic to protect consumers, their networks, and the messaging ecosystem from unwanted messages.[22] These industry best practices are one of the major reasons that providers' voluntary efforts have—as the Commission has observed—"gone a long way to protect consumers" from spam and scam text messages.[23]

The unconditional content-neutral and non-discriminatory blocking standard that non-consumer message senders seek[24] would effectively require that the wireless messaging industry scrap those best practices and unleash on consumers a torrent of unwanted messages,

---

[19] *Id.* at 3 (footnote omitted).

[20] *See generally, e.g.*, CTIA, *Messaging Principles and Best Practices* (May 2023) ("Messaging Principles and Best Practices"), https://api.ctia.org/wp-content/uploads/2023/05/230523-CTIA-Messaging-Principles-and-Best-Practices-FINAL.pdf; CTIA, *Messaging Security Best Practices* (June 2022) ("Messaging Security Best Practices"), https://api.ctia.org/wp-content/uploads/2022/06/Messaging-Security-Best-Practices-June-2022.pdf.

[21] *See* CTIA Comments at 7–8, 15–16, 18–19.

[22] *See, e.g.*, Messaging Principles and Best Practices at 20–22 §§ 7.1–7.2; Messaging Security Best Practices at 4 § 3.1.

[23] *Second Report and Order* ¶ 15.

[24] REACH Comments at 2; INCOMPAS Comments at 6–7; VON Comments at 6–7.

including messages related to illegal substances and content related to sex, hate, alcohol, firearms, and tobacco ("SHAFT" content).[25] Importantly, the industry's guidelines and best practices currently factor in whether message content is appropriately age gated. As a result, these best practices often serve as the primary line of defense in preventing children from receiving messages about controlled substances or containing adult content.[26] In fighting to eliminate these best practices, these non-consumer message senders are comparable to the illegal robocallers that the Commission is fighting hard to get "off the line."[27]

Other arguments for restricting current spam-prevention efforts are factually inaccurate and legally insufficient. VON, for example, suggests that the messaging ecosystem applies polices and processes in a haphazard, discriminatory manner.[28] This is incorrect, plain and simple. The messaging industry's best practices, and the policies and processes to implement them, apply in the same manner to *all non-consumer message senders*, regardless of the originating provider or channel used to send text messages. Indeed, wireless providers apply these same best practices to their own non-consumer message sender customers. The objective

[25] Other types of unwanted messages may include high-risk financial services, third-party lead generation, debt collection and forgiveness, gambling, and "get rich quick" schemes or multi-level marketing. *See, e.g.*, AT&T, AT&T Code of Conduct for AT&T Short Code and 10-Digit A2P SMS Messages at 6, 9–12 (Mar. 1, 2021) ("AT&T Code of Conduct"), https://docs.intelepeer.com/Atmosphere/Content/Resources/Files/att_bulk_messaging_code_of_conduct_re_10dlc_a2p_messages__03.2.pdf; T-Mobile, Code of Conduct (Version 2.2) at 18–19 (Nov. 2020) ("T-Mobile Code of Conduct"), https://www.t-mobile.com/support/public-files/attachments/T-Mobile%20Code%20of%20Conduct.pdf.

[26] *See* Messaging Principles and Best Practices at 14–15 § 5.3.1 (encouraging message senders to "monitor and prevent Unwanted messages and content, including for example content that . . . does not meet age-gating requirements."); T-Mobile Code of Conduct at 20; AT&T Code of Conduct at 10–11.

[27] *Robocall Response Team: Combating Scam Robocalls & Robotexts*, FCC, https://www.fcc.gov/spoofed-robocalls (last updated Aug. 18, 2022); *see* Press Release, FCC, FCC Announces Outcome of Coordinated Action Taken with FTC to Combat International Robocalls (Jan. 30, 2024), https://docs.fcc.gov/public/attachments/DOC-400143A1.pdf (highlighting FCC efforts "Getting Results" on combatting robocalls regarding auto warranty scams, student loan scams, and predatory mortgages).

[28] VON Comments at 3–6.

of the non-consumer campaign registries, like The Campaign Registry, is to ensure that non-mobile network operator ("MNO") text senders apply the same standards the MNOs themselves apply. And the Commission has noted that providers can and are expected to continue blocking based on these policies.[29]

To the extent that VON is objecting to more stringent standards for non-consumer message senders than consumer message senders,[30] its arguments do not hold up. Non-consumer message senders are demonstrably more likely to originate unwanted messages, and industry standards rationally protect against this. To "level [the] playing field,"[31] VON would have the Commission either (a) lower the standards for non-consumers that would result in bombarding consumers with unwanted text messages or (b) unnecessarily raise the bar for hundreds of millions of consumers to access mobile wireless services, impairing access by people with disabilities, older Americans, and other communities. Either way, consumers would suffer the consequences of VON's approach.

VON and REACH also ask the Commission to step in and oversee the industry's current text-blocking efforts, but their requests lack merit.[32] VON's argument that the Commission can and should regulate text-blocking measures because "[t]ext messaging uses NANP numbering" is reductionist to a fault.[33] As but one example, some OTT messaging platforms also use NANP numbers[34]—but VON makes no mention of these information services.

---

[29] *Second Report and Order* ¶ 19.

[30] VON Comments at 7.

[31] *Id.* at 2.

[32] *Id.* at 2–3, 9–10; REACH Comments at 5–6.

[33] VON Comments at 9.

[34] *See* Comments of CTIA, CG Docket No. 21-402, at 16 (filed Nov. 10, 2022) ("Some OTT applications are used exclusively over the Internet and use IP addresses for routing. Others provide users with

It is clear that VON and REACH would have the Commission adopt a framework with one endgame in mind: to allow their non-consumer message sender member companies to send more texts messages that consumers do not want.[35] This framework would lead to one result: making text messaging significantly less valued and trusted by American consumers.

IV. THE RECORD CONTINUES TO DEMONSTRATE THAT EFFECTIVELY MITIGATING SPAM AND SCAM TEXT MESSAGES REQUIRES A FRAMEWORK UNIQUE TO THE TEXT MESSAGING ECOSYSTEM.

A. The Commission Should Focus on Stopping Bad Actor Message Senders.

The Commission's proposal to require originating providers to block certain text messages would fail to effectively limit illegal text messages because an originating provider (a term undefined in the *Second FNPRM*) is not the "choke point" for all illegal messaging traffic generated by a message sender. The fact remains that bad actors are adept at spreading their traffic among multiple providers. Thus, the Commission should instead focus any blocking obligations on message senders.[36]

Further, the Commission should reject proposals to require terminating providers to block *all* traffic from originating providers due to the risk of over-blocking legitimate and wanted text messages.[37] Such a drastic approach would unnecessarily harm legitimate message senders and providers who may be unknowingly sending bad traffic.[38]

---

telephone numbers that allow messages to be exchanged between telephone numbers and Internet endpoints.").

[35] Consumer Advocates agree. *See* Consumer Advocates Ex Parte at 2.

[36] Twilio Comments at 6–7; CTIA Comments at 11–13.

[37] *See, e.g.*, NCLC Comments 5–8.

[38] *See, e.g.*, Twilio Comments at 6 ("[B]ad actors typically do not register their traffic and, instead, rely on [account takeovers] to use numbers registered to legitimate senders.").

B. No Further Commission Action Is Needed on Text Authentication Solutions.

Commenters continue to make clear that text messaging, unlike voice services, inherently incorporates a significant degree of authentication, and there is not the same "gap" for regulation to fill.[39] To the extent technical solutions for authenticating text messages can be developed, the Commission should continue to monitor the progress of technical experts at ATIS and others without imposing unnecessary reporting burdens on industry.

Further, there is consensus in the record that the predominant sources of spam text messages do not involve *number* spoofing but *identity* spoofing—that is, scams based on impersonation of brands or government agencies.[40] Verizon explains that "[w]hen bad actors impersonate legitimate enterprises using text messages, they generally use the text of the message or a malicious url as the main way to trick customers"[41] and demonstrates the challenges that providers face when applying new techniques to screen for and block identity spoofing schemes as bad actors evolve their tactics to evade providers' efforts to root them out.[42] Instead, targeting bad actors with law enforcement action is the best way to tackle this problem. For example, the Commission should partner with the FTC, which has recently adopted a trade regulation rule against impersonation of government agencies or business entities and proposes to extend that rule to prohibit impersonation of individuals.[43]

---

[39] Verizon Comments at 5 ("[T]here is simply not a problem to solve when it comes to spoofing numbers for SMS and MMS."); Twilio Comments at 8; *see also* CTIA Comments at 22–23 & n.63.

[40] Comments of Campaign Verify at 1; Twilio Comments at 7–8; Comments of NetNumber at 4; Verizon Comments at 5.

[41] Verizon Comments at 5.

[42] *Id.* (describing an example of efforts by bad actors to circumvent new blocking and screening techniques for enterprise names).

[43] Trade Regulation Rule on Impersonation of Government and Businesses, 89 Fed. Reg. 15017 (Mar. 1, 2024) (to be codified at 16 C.F.R. pt. 461); Trade Regulation Rule on Impersonation of Government and Businesses, 89 Fed. Reg. 15072 (Mar. 1, 2024).

C. The Commission Should Avoid Stranding Legitimate Users of Email-to-Text.

CTIA and its member companies recognize that the email-to-text service has been used as a vector for spam and scam, and the record demonstrates that providers are taking increasingly effective steps to protect consumers from these harms.[44] However, the Commission's proposal to make email-to-text service opt-in is overbroad and would risk stranding the many legitimate users of the service, including federal, state, and local governments and public safety agencies. One CTIA member reports that over 300 financial institutions use email-to-text service to reach customers—just one example of the many legacy users that rely on the platform and may need to be transitioned more gradually. Instead, the wireless industry would welcome the Commission's efforts to minimize the use of the email-to-text service by encouraging such users to migrate to other non-consumer messaging channels with more robust anti-spam and scam protections.[45]

D. CTIA's Secure Messaging Initiative is Ready as a Resource for "Traceback."

Multiple commenters recognize that a voluntary, industry-led effort would be the most effective way to implement a "traceback" process for text messaging.[46] Through CTIA's SMI, industry stakeholders are already collaborating with enforcement partners on a voluntary basis. The record confirms that the SMI can and should serve as the Commission's resource for collaborative efforts and information sharing about bad actors to help the wireless industry, government agencies, and the Commission harness their collective resources to better target bad actors.[47]

---

[44] CTIA Comments at 24; Verizon Comments at 6.

[45] Verizon Comments at 7–8.

[46] Verizon Comments 5–6; Twilio Comments at 7; VON Comments at 8; NetNumber Comments at 2–5.

[47] Verizon Comments at 6; Twilio Comments at 7.

V. CONCLUSION.

As the record demonstrates, the wireless industry is dedicated to protecting consumers from spam text messages and is engaged in strong collaboration throughout the messaging ecosystem to do so. The Commission should avoid calls by non-consumer message sender advocates to undo the significant progress that providers have made and, in applying "content neutral" and "non-discriminatory" blocking standards, unleash a flood of spam and scam text messages on consumers. The Commission should also recognize that the robocall playbook is not the appropriate framework for the text messaging ecosystem and should focus its efforts on enhancing coordination and enforcement efforts with industry, including through the SMI. These efforts will better achieve the Commission's goals to protect consumers from spam text messages.

Respectfully submitted,

/s/ Sarah Leggin
Sarah Leggin
Assistant Vice President, Regulatory Affairs

Thomas C. Power
Senior Vice President and General Counsel

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

Mike Beirne
Director, Regulatory Affairs

CTIA
1400 Sixteenth Street, N.W.
Suite 600
Washington, D.C. 20036
(202) 736-3200

March 11, 2024