

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

In the Matter of)	
)	
Rules and Regulations Implementing the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003)	CG Docket No. 04-53
)	
Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991)	CG Docket No. 02-278
)	

COMMENTS OF NEXTEL COMMUNICATIONS, INC.

Celeste M. Moy
Vice President and
Assistant General Counsel
Frank Triveri
Special Counsel
NEXTEL COMMUNICATIONS, INC.
2001 Edmund Halley Drive
Reston, VA 20191
(703) 433-4000

To-Quyen T. Truong
Jason E. Rademacher
Courtney Manzel
DOW, LOHNES & ALBERTSON, PLLC
1200 New Hampshire Avenue, NW
Suite 800
Washington, DC 20036
(202) 776-2000

Its Attorneys

April 30, 2004

TABLE OF CONTENTS

	Page
SUMMARY.....	i
INTRODUCTION & SUMMARY	1
BACKGROUND.....	2
DISCUSSION.....	4
I. THE COMMISSION SHOULD MAINTAIN A LIST OF RESTRICTED MOBILE MESSAGE DOMAIN NAMES TO WHICH MARKETERS CAN REFER TO COMPLY WITH THE ACT.	4
A. An MSCM Domain Name List Would Be the Most Effective Means to Give Senders the Ability to Comply With the Act.....	4
B. The Alternative Addressing Schemes Would be Inefficient and Would Overburden Wireless Providers and Consumers	5
II. REQUIRING CARRIERS TO IMPLEMENT A CHALLENGE-RESPONSE CAPABILITY WOULD PLACE INAPPROPRIATE BURDENS ON CARRIERS AND THEIR NETWORKS.....	8
A. The Act Does Not Authorize the Commission To Impose Primary Compliance Responsibility on Carriers.	9
B. Even After Imposing Substantial Unjustified Costs on Wireless Providers, a Challenge-Response Requirement Still Would Not Stop Problem Spammers.	12
III. THE CAN SPAM ACT REQUIRES PRIOR AUTHORIZATION TO SEND MSCMs..	15
IV. THE COMMISSION SHOULD ADOPT AN EXCEPTION TO ALLOW MOBILE CARRIERS TO COMMUNICATE WITH THEIR OWN SUBSCRIBERS.....	16
CONCLUSION.....	21

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

In the Matter of)
)
Rules and Regulations Implementing the) CG Docket No. 04-53
Controlling the Assault of Non-Solicited)
Pornography and Marketing Act of 2003)
)

To: The Secretary

COMMENTS OF NEXTEL COMMUNICATIONS, INC.

Nextel Communications, Inc. (“Nextel”), by its attorneys, hereby submits these Comments in response to the Federal Communications Commission’s (“FCC’s”) *Notice of Proposed Rulemaking*¹ on how best to implement the provisions of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (the “CAN-SPAM Act” or the “Act”)² to prevent unwanted mobile service commercial messages (“MSCMs”) on wireless devices.

INTRODUCTION & SUMMARY

As a leading provider of mobile messaging services to consumers and businesses nationwide, Nextel has a substantial interest in ensuring that wireless networks remain as free as possible of mobile spam. Towards that end, Nextel fully supports the implementation of the CAN-SPAM Act to maximize wireless customers’ and operators’ freedom from unwanted mobile messages, while minimizing the burdens on wireless networks and consumers’ right to receive mobile messages from sources they welcome. The adoption of an opt-in regime for

¹ Rules and Regulations Implementing the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, *Notice of Proposed Rulemaking and Further Notice of Proposed Rulemaking*, CG Docket No. 04-53, CG Docket No. 02-278, 69 Fed. Reg. 16873 (rel. Mar. 19, 2004) (the “Notice”).

² Pub. L. No. 108-187, 117 Stat. 2699 (2003), *to be codified at* 15 U.S.C. § 7701, *et seq.*

wireless messaging is an important step toward these goals. Nextel submits these Comments in an effort to aid the Commission's development of other effective and efficient measures to satisfy these public policy goals and statutory mandates.

Congress designed the Act to provide an efficient framework to protect consumers and networks from the burdens and costs of unwanted MSCMs, by requiring the senders of those electronic messages to take certain compliance actions. The Act does not impose and does not authorize the imposition of complex and costly anti-spam mandates (such as the proposed "challenge-response" mechanism) that apportion primary compliance responsibility and costs to wireless carriers – and, ultimately – to consumers. Instead, the Act requires the senders of mobile messages to bear the compliance responsibility and costs for the messages that they send and from which they reap the economic return.

The simplest and most efficient way for the Commission to implement the Act's MSCM provisions is to develop a list of the domain names that carriers use exclusively for mobile messaging, and require senders of commercial emails to consult that list and delete from their mailing lists any electronic addresses that include a wireless domain name. In contrast, requirements such as the "challenge-response" blocking proposal would be cumbersome and ineffective, and ultimately would harm consumers through increased costs, service delays and threats to their privacy.

The Commission should implement an opt-in regime for MSCMs, as the CAN-SPAM Act requires. Conversely, pursuant to Section 14(b)(1), the Commission should exempt wireless carriers' communications with their own customers from the MSCMs regulated by the Act, so long as the customers are not charged for these communications.

BACKGROUND

Nextel operates a nationwide digital mobile network that provides more than 13 million consumer and business customers with an array of fully-integrated, all-digital wireless communications services, including digital mobile telephone service, two-way radio service, and mobile messaging. Nextel also offers its customers a bundle of wireless Internet access and related Web services including advanced Java-enabled business applications. Using Nextel's Internet-enabled handsets, customers can search the Internet, access wireless websites, send and receive messages, and access office email accounts, events and calendar lists.

As a provider of mobile messaging services, Nextel shares Congress's concern for protecting its subscribers as well as its network from the scourge of wireless spam. The CAN-SPAM Act defines MSCMs as "commercial messages," thus subjecting them to the requirements of and prohibitions on general unsolicited commercial email ("UCE"). In addition, Section 14 of the Act specifically targets commercial messages to mobile messaging accounts. In Section 14(b) of the Act, Congress specifically directs senders to provide MSCMs only to consumers who have expressly consented to receiving those messages. Notably, Congress imposed no duty on mobile messaging service providers to police sender conduct or to block improper MSCMs. To the contrary, by directing the FCC to "determine how a sender of [MSCMs] may comply with the provisions of this Act," Section 14(b)(4) squarely places the responsibility of complying with the Act on *senders* of MSCMs. Senders face civil and/or criminal penalties under the Act for ignoring this requirement, including monetary forfeiture and imprisonment.³ Indeed, both the Act and the legislative history focus on the message sender's relationship with the recipient and

³ CAN-SPAM Act, §§ 4, 5.

the sender's regulatory obligation. At no point did Congress contemplate imposing compliance obligations on providers of email and wireless messaging services.⁴

DISCUSSION

I. THE COMMISSION SHOULD MAINTAIN A LIST OF RESTRICTED MOBILE MESSAGE DOMAIN NAMES TO WHICH MARKETERS CAN REFER TO COMPLY WITH THE ACT.

To implement the Section 14(b) prohibition on sending MSCMs without the recipients' express prior consent, the Commission proposes several solutions that will enable senders to ascertain whether they are sending messages to a wireless messaging account. These include developing a list of mobile messaging domain names, compiling a registry of individual mobile subscriber addresses, requiring carriers to use a common mobile messaging-only domain name, and requiring carriers to use common mobile messaging subdomain names.⁵

A. An MSCM Domain Name List Would Be the Most Effective Means To Give Senders the Ability to Comply With the Act.

The most effective way to stop senders from unknowingly sending wireless spam is to create a database of domain names that carriers use exclusively for mobile messaging. To avoid violating the Act, marketers would consult the domain name list to determine whether the electronic addresses to which they intend to send MSCMs are actually mobile messaging addresses. This approach would satisfy Congress's concerns that the message sender have a reasonable means to identify mobile messaging addresses for compliance purposes.⁶

⁴ *Id.*; see also, e.g., 149 Cong. Rec. H12186, 12194 (“[This bill] requires marketers to let people know who they are and where they can be located. . . It prohibits marketers from deceiving consumers. . .”) (statement of Rep. John Dingell).

⁵ *Notice*, ¶¶ 27-31.

⁶ CAN-SPAM Act, § 14(c).

One of the chief virtues of a domain name list would be its ease of administration. Much like the Do-Not-Call List in the telemarketing context, a domain name list would create a simple source for businesses to consult and determine whether a particular commercial message is permitted or proscribed by the CAN-SPAM Act. Similarly, the list would conserve the resources of the Commission and other enforcement authorities by providing a clear-cut test for determining whether a sender should have known that it was sending a commercial message to a mobile messaging address. With a mobile messaging domain name list, spammers could raise no legitimate claim that they lack a reasonable way to identify a recipient's mobile messaging address.

The domain name list approach also would give wireless providers a quick and inexpensive way to protect customers from unwanted MSCMs. Under this regime, wireless providers would report their mobile messaging domain names for inclusion on the list and provide updates if they discontinue or add any domain names. The domain name list approach best achieves Congress's goal to eliminate wireless spam because it provides the most efficient and reasonable way for MSCM senders to identify mobile messaging addresses, and it places primary responsibility on those who can best ensure compliance: the senders of commercial messages.

B. The Alternative Addressing Schemes Would Be Inefficient and Would Overburden Wireless Providers and Consumers.

By comparison to the domain name list approach, the alternative proposals to require carriers to alter existing wireless messaging domain or subdomain names or to implement a Do-Not-Message directory would be severely disruptive and inefficient.⁷

⁷ Notice, ¶¶ 30-31.

A requirement that all carriers use the same domain or subdomain names for their mobile messaging addresses would force every carrier to change its existing customer addresses and domain name conventions. This conversion would require carriers to undertake extensive, costly and time-consuming computer system changes and customer care campaigns.

First, carriers' internal message routing systems refer to the domain names in mobile messaging addresses to properly relay messages to their intended recipients in a fast and efficient manner. Accordingly, carriers would have to update their databases and change their many internal system codes and parameters just to accommodate new domain or subdomain names for all mobile messaging addresses.

Second, carriers would need to conduct large-scale customer care campaigns to contact and inform their customers of the change in their mobile messaging addresses. Such a change also would trigger a high volume of calls to carriers' customer support representatives, as customers seek clarification and troubleshooting from their carrier, or to lodge complaints regarding the disruption caused by the address changes. A carrier such as Nextel would have to spend millions of dollars to implement these changes, thus diverting scarce carrier resources from other beneficial activities, such as the roll-out of new technology and other improvements in customer service. The disruption caused by such a change would only frustrate customers, and thus undermine the wireless industry's and the Federal Government's mutual goal of promoting advanced communications services.

Customers also would incur substantial added costs and annoyances if they are forced to change their mobile messaging contact addresses. Businesses that rely on automated volume messaging to their employees would have to accommodate burdensome changes in naming conventions. Every mobile messaging customer would have to notify all senders of their new

addresses, and customers inevitably would fail to communicate the change to some parties with whom they wish to correspond. The costs would be particularly severe for small businesses and individuals who depend on well-established electronic addresses to offer instant accessibility to their customers. In other contexts, the Commission has noted the costs to customers of changing their contact information,⁸ and the costs imposed in this circumstance would be no different. Given Congress' purpose of providing special protection to wireless messaging customers from the expense and annoyance of MSCMs, requiring those same customers to bear the costs and dislocation involved in changing the domain names of their wireless messaging accounts would flatly contradict Congress's intent.

Moreover, requiring the use of universal domains or subdomains could prove to be an unwise technological choice. Electronic address conventions may change over time, and the FCC should allow carriers flexibility to adapt to such changes. If the Commission adopts a universal domain name requirement and then is forced by future technical developments to change its domain names again, carriers and customers would be forced to bear the same costs multiple times. There is no evidence that Congress intended to impose these costs on carriers and customers when it adopted the wireless provisions of the CAN-SPAM Act, and there is no justification for imposing those costs on carriers and customers to correct a problem that unscrupulous spammers have created – particularly when the less burdensome domain name list

⁸ See, e.g., Verizon Wireless's Petition for Partial Forebearance From the Commercial Mobile Radio Services Number Portability Obligation and Telephone Number Portability, *Memorandum Opinion and Order*, WT Docket No. 01-184, CC Docket No. 95-116, FCC 02-215 (rel. July 26, 2002), *Petition for Review denied*, 356 U.S. App. D.C. 238 (D.C. Cir. 2003).

approach provides a “narrower alternative that has all the same advantages and fewer disadvantages,”⁹ and provides the additional benefit of protecting privacy.

In comparison with the proposed Do-Not-Message Directory,¹⁰ a domain name list approach would obviate the need for publication of consumers’ mobile messaging addresses any more widely than necessary to stop unwanted MSCMs. Nextel takes the issue of customer privacy very seriously, as does the Commission,¹¹ and the domain name list approach is the most effective way to protect that interest.

II. REQUIRING CARRIERS TO IMPLEMENT A CHALLENGE-RESPONSE CAPABILITY WOULD PLACE INAPPROPRIATE BURDENS ON CARRIERS AND THEIR NETWORKS.

The Commission seeks comment on whether carriers should employ a “challenge-response” capability to identify, quarantine, challenge and block individual MSCMs pending confirmation by the sender that the message is intended to be delivered to a mobile messaging subscriber.¹² In scope, this challenge-response requirement would be akin to requiring local exchange carriers to monitor all incoming calls to each of their customers and to block any unwanted telemarketing calls. Certainly no one could contemplate such a scheme for implementing the Do-Not-Call regulations, and there is no basis for implementing anything

⁹ See *United States Telecom Association v. F.C.C.*, F.3d 554, 571 (D.C. Cir. 2004) (holding that “a rule is irrational if a party has presented to the agency a narrower alternative that has all the same advantages and fewer disadvantages and the agency has not articulated any reasonable explanation for rejecting the proposed alternative.”).

¹⁰ Notice, ¶ 29.

¹¹ See, e.g., Implementation of the Telecommunications Act of 1996; Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information, *Second Report and Order and Further Notice of Proposed Rulemaking*, CC Docket No. 96-115, FCC 98-27, 63 Fed. Reg. 20326 (rel. Feb. 26, 1998).

¹² Notice, ¶ 32.

similar in the mobile messaging context. A challenge-response requirement would assign primary compliance responsibility to mobile carriers. Such a regime would contravene Congress's intent to place the compliance obligation on potential violators (*i.e.*, MSCM senders), and not on victims (*e.g.*, carriers who would otherwise face unnecessary network costs). The challenge-response approach also would be excessively costly and ineffective in comparison to the domain name list system.

A. The Act Does Not Authorize the Commission To Impose Primary Compliance Responsibility on Carriers.

Placing the burdens of a challenge-response regime on wireless operators would contravene the CAN-SPAM Act and its legislative history. The CAN-SPAM Act focuses on the relationship between the senders of commercial messages and their recipients, and relies on that framework to establish senders' compliance obligations and liabilities.¹³ Specifically, Section 14 directs the Commission to determine how *senders*, not wireless carriers, can comply with the Act's limitations on MSCMs.¹⁴ The only portion of the Act that places any compliance obligation on wireless carriers is Section 14(b)(3), which requires carriers to abide by the provisions of the Act when they act as *senders communicating with their customers*. Even here, the Act gives the Commission the option of partially exempting carriers from compliance.¹⁵ The

¹³ For example, the Act's penalties are imposed on parties that "send" or "initiate" improper UCEs and MSCMs. CAN-SPAM Act, §§ 4, 5. Under the Act, to be a "sender" of a UCE or MSCM, a party must both "initiate" it, and have its products advertised thereby. *Id.*, § 3(16). Accordingly, the Act does not punish service providers for delivering electronic messages initiated by others.

¹⁴ CAN-SPAM Act, §§ 14(b)(4), 14(c).

¹⁵ Section 14(b)(3) directs the FCC to consider making an exception for messages sent by wireless carriers to subscribers. Carriers would not be required to obtain authorization from the subscriber before sending the message, but would be required to honor any opt-out requests.

Act reflects Congress' recognition that compliance responsibility or liability should not attach to network operators who merely serve as a conduit for messages.¹⁶

Far from seeking to impose additional obligations and costs on messaging service providers, Congress expressed its intent to prevent marketing messages from overburdening service providers and their networks. In recounting the Congressional Findings and Policy underlying the statute, Section 2 of the Act acknowledges that “[t]he growth in unsolicited commercial electronic mail imposes significant monetary costs on providers of Internet access services, businesses . . . that carry and receive such mail, as there is a finite volume of mail that such providers . . . can handle without further investment in infrastructure.”¹⁷ Likewise, the initial sponsor of the wireless provisions, Congressman Markey, stated that Section 14 was designed to tackle wireless spam “before it overwhelms users and network operators alike.”¹⁸ Congress noted the strains that spam places on service providers' networks and recognized that the resulting costs will be passed on to consumers in the form of higher service rates.¹⁹

Congress observed with approval the blocking strategies employed by both Internet service and wireless messaging providers.²⁰ The drafters did not, however, require the continued employment of such strategies or the initiation of new ones by network operators, given these providers' strong economic incentives to prevent unwanted commercial messages from

¹⁶ See CAN-SPAM Act, §§ 3(9), (15) (exempting “routine conveyance” from the definition of “initiate”); S. Rep. 108-102 at 15 (2003) (“However, the definition specifies that a company that merely engages in routine conveyance, such as an ISP that simply plays a technical role in transmitting or routing a message and is not involved in coordinating the recipient addresses for the marketing appeal, shall not be considered to have initiated the message.”).

¹⁷ CAN-SPAM Act, § 2(a)(6).

¹⁸ 149 Cong. Rec. H12860.

¹⁹ S. Rep. No. 108-102 at 2-3, 6-7.

²⁰ See, e.g., 149 Cong. Rec., at H12194.

overwhelming their networks. Instead of imposing new burdens, Congress provided ISPs with tools to combat spammers that include the ability to seek civil remedies from offending senders.²¹

Nextel has made the most of these tools, combining legal and technical solutions to engage in a “full-court press” on spammers. In October, 2003, Nextel launched the most advanced version of its spam filtering technology.²² This technology relies on a highly sophisticated statistical filtering methodology that analyzes all aspects of a message to identify and delete spam. Most significantly, this intelligent technology builds on the information that it processes and improves spam detection capabilities over time. Overall, the filter has dramatically reduced the amount of spam that reaches Nextel’s subscribers.

Not content with just this technical solution, Nextel has pursued spammers, serving cease and desist notices, and filing suit when spammers have chosen to ignore Nextel’s warnings.²³ The strong economic incentives to satisfy customers ensure that carriers like Nextel employ the most effective mix of solutions to rid its network of spam. As victims, carriers have every incentive to deploy spam reduction solutions, and are positioned to know what works best and

²¹ CAN-SPAM Act, § 7(g). *See also, e.g.*, 18 U.S.C. § 1030.

²² Both the Electronic Communications Privacy Act, 18 U.S.C.A. § 2701, *et seq.*, and the Communications Act of 1934, 47 U.S.C.A. § 230, empower carriers to utilize such tools.

²³ Nextel has relied on Federal and state laws that prohibit computer fraud and abuse, *see, e.g.*, 18 U.S.C.A. §1030), computer trespass, and trademark infringement (the Lanham Act, 15 U.S.C.A, § 1051, *et. seq.*) to combat spam. *See, e.g.*, Nextel Communications Inc., a Delaware Corporation, and Nextel South Corp., a Georgia corporation v. Nicholas Stewart, iDENcustom, and John Does 1-100, inclusive, In the U.S. District Court for the Northern District of Georgia, Atlanta Division, C.A. No. 1-04-CV-1084; *and see* Nextel Communications Inc., a Delaware Corporation, and Nextel South Corp., a Georgia corporation v. Gerald Arnone, Sharon Ruby, ENYO Communications Inc., and John Does 1-100, inclusive, In the U.S. District Court for the Northern District of Georgia, Atlanta Division, C.A. No. 1-03-CV-4008-RWS.

how to allocate scarce resources. Indeed, Nextel's efforts to date demonstrate precisely why the Commission must not impose burdensome obligations on network operators. Imposing on carriers costly, burdensome government mandates like a challenge-response mechanism would only frustrate the deployment of the most efficient and effective solutions available.

B. Even After Imposing Substantial Unjustified Costs on Wireless Providers, a Challenge-Response Requirement Still Would Not Stop Problem Spammers.

The proposed challenge-response scheme also would place unfair burdens on wireless carriers' wireline message delivery infrastructure without eliminating wireless spam. A basic challenge-response process would multiply by between two and four times the number of transmissions involved each time a sender tries to transmit a commercial mobile message. First, when the sender attempts to contact the intended recipient, presuming the mobile service provider could tell that the message is for a commercial purpose, the provider would detect, then quarantine the message. Second, the provider would send a message to notify the sender that it has routed an MSCM to a mobile messaging address. Third, the sender would notify the mobile service provider as to whether the provider should deliver the message to the recipient. Fourth, receipt of an affirmative response from the sender would cause the mobile service provider to forward the message to the intended recipient. Thus, a challenge-response mechanism will replace one MSCM with up to four associated messages. When that increased burden is multiplied by the quantities typical of mass commercial messaging, the burden on carrier infrastructure becomes staggering.

There are numerous other hidden problems and costs associated with a challenge-response regime that make it both unfair and unworkable. Introducing a challenge-response procedure would require most carriers to completely overhaul their current email handling procedures to (a) identify commercial messages, (b) route and quarantine such messages in

queue, (c) conduct the challenge-response exchange, and (d) delete or reroute messages based on the sender response. Because carriers do not have automated systems that would provide a streamlined challenge-response process at this time, carriers would have to carry out many of these functions manually. Given the volume of commercial messages received on a regular basis, manual treatment would be cost prohibitive. It also would be highly inequitable for the Commission to require carriers to overhaul their email processing and routing software in order to develop automated systems to combat MSCMs.

The challenge-response scheme would also place considerable burdens on both mobile carriers and senders of MSCMs. The processing and transmission demands of the challenge-response scheme would raise carriers' costs as messaging volume increases. For instance, during periods of increased network traffic, carriers would be forced to quarantine commercial messages for a longer period of time in order to complete the challenge-response process, requiring costly, additional server space.²⁴ In addition, because the challenge-response exchange between the carrier and the sender can overwhelm the email system and personnel resources of a small business that sends electronic messages in bulk, small entities that send commercial messages will be required to upgrade their internal systems to accommodate increased traffic under a challenge-response scheme. The Commission has shown a laudable concern for the interests of small businesses and the effects that its CAN-SPAM rules will have on them, but this proposal clearly will place unmanageable demands even on small businesses making every effort

²⁴ Nextel currently blocks 40% of the electronic messages it receives as spam every day, but it quickly deletes these messages.

to comply with the rules.²⁵ Thus, this regime thus would make it even harder for small businesses to operate an honest business.

At the same time, the challenge-response regime would be ineffective to block unscrupulous spammers, who have perfected many tools for avoiding detection and blocking. For example, the spammer may not use its own return address or may not provide a return address at all. If a spammer spoofed an unrelated third-party's electronic address, then the challenge messages could overload the email server of an unrelated, innocent party. Similarly, spammers can send emails using Internet Protocol addresses that do not permit emails to be directed to them.

A functional challenge-response system depends on senders who identify the message as having a commercial purpose.²⁶ To avoid a challenge, unscrupulous spammers are highly unlikely to include any identifier. But even if they did so, there is no reason to expect that spammers will have any compunction about answering in the affirmative when asked whether they have permission to send messages to a wireless subscriber. Equally alarming, spammers could use the challenge-response mechanism to compile lists of active mobile messaging numbers, in a scheme similar to that used by bulk email spammers.²⁷ Because only valid addresses would provoke a challenge from the wireless service provider, the spammer could use the challenges it receives to validate and compile a list of active mobile messaging addresses for future use or sale to other spammers.

²⁵ See, e.g., *Notice*, ¶¶ 23, 25, 28-32, 34, 36.

²⁶ *Id.*, ¶¶ 33-34.

²⁷ See, e.g., Brian Krebs, "FTC to Announce First Ever Crackdown on Spam," *Newsbytes*, Jan. 31, 2002 (FTC working on cases involving sham opt-out links that are used by spammers to verify consumers' email addresses for future spam).

There is no evidence that a challenge-response system would be more effective at stopping spam than the domain name list system. Certainly there is no indication that it would be so much more effective as to justify the attendant costs and the increased risk of abuse by unscrupulous spammers. Under these circumstances, the Commission lacks any basis in the statute or the evidence to impose the challenge-response regime rather than the domain name list system.

III. THE CAN SPAM ACT REQUIRES PRIOR AUTHORIZATION TO SEND MSCMs.

The CAN-SPAM Act requires senders to provide customers the “ability to avoid receiving [MSCMs] unless the subscriber has provided express prior authorization to the sender.”²⁸ Nextel agrees that the Act’s definition of “affirmative consent” should be the starting point for defining “express prior authorization,”²⁹ and that for MSCMs, express prior authorization means an affirmative act to “opt in” before the first message is sent. This approach is quite different than the “opt-out” regime that the CAN-SPAM Act establishes for traditional commercial electronic mail messages, but this differential treatment is justified due to the different natures of email and MSCMs. Congress no doubt understands the need for greater protections of wireless subscribers who, among other things, often pay per-message fees. The Commission should thus make clear that MSCM senders are prohibited from sending MSCMs without the wireless subscriber’s express prior authorization as required by the Act.

The Commission need not adopt a particular opt-in method or form.³⁰ Instead, it is enough that a subscriber manifest an affirmative desire to receive MSCMs from the sender.

²⁸ CAN-SPAM Act, § 14(b)(1).

²⁹ *Notice*, ¶ 35.

³⁰ *Id.*, ¶ 36.

Some action on the part of the subscriber should be required and may range from submitting written consent to clicking an “I accept” button on a web page. The burden of proving prior express consent should be on the sender. Thus, Nextel supports subscriber flexibility as to how consent is delivered or obtained.

The Commission should not exempt small businesses from the prior-express-authorization requirement.³¹ Spammers tend to be small businesses that try to reach large markets at the lowest cost. While many are reputable businesses, pornographers, scammers, and less reputable enterprises all would qualify as “small businesses;” thus any exemption would only exacerbate the problem.

In any event, the Act does not provide for an exemption for small businesses. Yet Congress did authorize the Commission to provide an exemption for wireless carriers that communicate with their customers. This strongly suggests that Congress intentionally did not exempt small businesses or others from any prior-express-authorization requirement.

IV. THE COMMISSION SHOULD ADOPT AN EXCEPTION TO ALLOW MOBILE CARRIERS TO COMMUNICATE WITH THEIR OWN SUBSCRIBERS.

Section 14(b)(3) of the Act permits the Commission to exempt commercial mobile radio service (CMRS) providers’ mobile message communications to their subscribers from the general prohibition against sending MSCMs without the recipients’ prior express consent.³² The Commission notes that transactional messages from CMRS carriers to their subscribers already are exempted from the coverage of the Act.³³ In some circumstances, however, the transactional message exemptions do not, on their face, go far enough to permit CMRS providers to

³¹ *Id.*, ¶¶ 23, 36.

³² *Id.*, ¶ 38.

³³ *Id.*, ¶ 39.

communicate freely with their customers. The FTC currently is considering issues related to the transactional email exception in its own CAN-SPAM Act rulemaking proceeding.³⁴ On matters that are within the agencies' concurrent jurisdiction, Nextel strongly encourages the FCC to consult with the FTC and provide the benefit of the FCC's expertise regarding the telecommunications industry.³⁵ With regard to the FCC's exclusive jurisdiction over CMRS carriers and their transmission of mobile messages to their subscribers, the Commission should exercise its full authority under Section 14(b)(3) in this proceeding to exempt such messages from the MSCM rules, so long as the CMRS carrier does not charge its subscribers for such messages.

The Act directs the Commission to evaluate the nature of the relationship between wireless messaging customers and CMRS providers in determining whether to exempt messages between them from the coverage of the Act.³⁶ The Commission recognized in the TCPA context that mobile carriers were free to contact their subscribers via autodialed or pre-recorded messages so long as subscribers are not charged for the transmission.³⁷ The Commission should

³⁴ Definitions, Implementation, and Reporting Requirements Under the CAN-SPAM Act, *Advance Notice of Proposed Rulemaking*, Project No. R4110008, 69 FR 11776 (rel. March 11, 2004).

³⁵ CAN-SPAM Act § 14(b). For example, the FCC should advise the FTC regarding the impracticability of transporting into the MSCM realm all email requirements (*e.g.*, inclusion of detailed physical address and opt-out information in a short mobile message, particularly if every advertiser whose product is included in the message must provide such information).

³⁶ *Id.*, § 14(b)(3).

³⁷ See Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, CC Docket No. 92-90, *Report and Order*, 7 FCC Rcd 8752, at 8775 (1992); See also Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, CG Docket No. 02-278, *Report and Order*, FCC 03-153 (2003), *summarized* 68 Fed. Reg. 44144 (July 25, 2003). While Nextel does not agree that the TCPA governs text messages, it agrees that sending such messages to a mobile device without that party's express prior authorization should not be permitted when the receiving party pays.

adopt a similar exemption in the MSCM context to facilitate the flow of useful information from carrier to subscriber when such communications create no additional costs for subscribers.

The ability to communicate with customers is vital in the highly competitive wireless services market where innovative new services and service plans are in constant development and customer churn occurs at a high rate. Typical wireless customers are highly interested in the service-oriented information carriers provide, and permitting them to opt out if they decide otherwise is sufficient. Moreover, wireless carriers are able to ensure that customers are not charged for the messages, unlike third parties that send unwanted or unsolicited messages.

The ability to communicate through mobile messaging with customers is especially important in the prepaid mobile services context, where such messages often provide the only dependable way for a carrier to communicate with customers, because the carrier generally does not have other reliable customer contact information. For example, Nextel's wholly-owned subsidiary Boost Mobile provides prepaid mobile services, which are marketed primarily to technologically savvy younger purchasers. Subscribers typically purchase a wireless phone with a certain number of prepaid minutes that can be used for an array of different functions including traditional voice service, two-way radio service, mobile messaging, and other data services. Customers' prepaid service time expires, regardless of whether it has been used, 90 days from the date service is activated. Remaining service time, however, is added to a new 90-day period if the customer purchases an additional amount of prepaid service.

Many prepaid customers submit dummy personal contact information because prepaid service activation requires only accurate identifying information regarding the phone and phone card purchased by the customer, and additional contact information is not needed for regular billing. In some cases, dealers activate the phones before sale so that they can offer them to

customers as “ready-to-use” and, as a result, the information they provide does not properly identify the actual purchaser of the phone and service. Accordingly, Boost’s review of its customer contact information consistently shows extensive inaccuracies in the customer name, wireline phone, email and physical address entries.

Nonetheless, Boost occasionally needs to contact its prepaid customers to provide important information, including notification of changes in available service functions, coverage or rates. In addition when a customer’s prepaid service is about to expire, Boost must notify customers of their remaining service time and the need to “re-Boost” if the customer wishes to maintain service beyond the existing 90-day service period. Such notice is particularly important to customers who purchase prepaid service primarily for security and emergency use, or strictly for two-way radio use, and may be unaware or may forget that their service will expire even though they have not used up their airtime during the 90-day service period. In other cases, some customers may have exhausted their airtime, so that they are not even accessible through Boost’s mobile voice service, and Boost’s free incoming mobile messaging service provides the only means to reach the customer. In short, due to the dearth of reliable contact information, the only effective way to reach prepaid mobile service customers is through mobile messaging.³⁸ The prepaid mobile service scenario thus demonstrates the efficacy and importance of mobile messaging for communication from wireless service providers to their subscribers.

As explained above, Congress considered mobile carriers to be among the victims, rather than the instigators, of the mobile spam problem. Because mobile spam threatens the long-term

³⁸ Although these messages may generally fit within the transactional email exception in Section 3, this determination is often difficult to make in light of the commercial element in some of the messages.

viability of mobile messaging services, CMRS providers have a strong economic incentive to avoid wasting their scarce network resources on the transmission of unwanted messages to their subscribers, and they have invested heavily in voluntary blocking mechanisms and other means to combat wireless spam. Mobile carriers such as Nextel are acutely aware of the frustration that repeated commercial messages cause in customers. Carriers therefore have a strong customer-service based incentive to avoid abusing an exemption that would allow them to communicate with their subscribers. Because the exemption would apply only to messages for which carriers do not charge their subscribers, such messages represent an unrecoverable cost, giving carriers a further financial incentive to avoid sending large numbers of MSCMs.

Finally, the Act provides a ready mechanism for honoring subscriber preferences even when mobile messages sent by CMRS carriers to their subscribers are exempt from the prior-express-authorization requirement. If the Commission adopts this exemption, CMRS carriers would be subject to the Section 14(b)(3) self-activating requirement that they “allow their subscribers to indicate a desire not to receive future mobile service commercial messages from the provider (1) at the time of subscribing to such service, and (2) in any billing mechanism.”³⁹ When customers have not opted out, however, the Commission should protect the flow of beneficial information from mobile carriers to subscribers by exempting from Section 14 of the Act all mobile messages sent by CMRS carriers to their subscribers, so long as the carriers do not impose a charge on their subscribers.

³⁹ CAN-SPAM Act, § 14(b)(3). This opt-out right would approximate the rules governing email service providers under the non-wireless provisions of the CAN-SPAM Act. *Id.*, § 5(a)(4).

CONCLUSION

As a provider of mobile messaging services, Nextel has a strong interest in ensuring the success of the CAN-SPAM Act and the end of widespread spamming. The way to accomplish that is not by imposing unjustified costs on wireless providers and their subscribers but by actively pursuing and prosecuting spammers. Nextel's regulatory approach will aid the Commission in facilitating prosecution, while providing honest marketers the compliance tools they need. Accordingly, Nextel respectfully requests that the Commission adopt the regulatory proposals described herein.

Respectfully submitted,

Celeste M. Moy
Vice President and
Assistant General Counsel
Frank Triveri
Special Counsel
NEXTEL COMMUNICATIONS, INC.
2001 Edmund Halley Drive
Reston, VA 20191
(703) 433-4000

/s/ To-Quyen T. Truong
To-Quyen T. Truong
Jason E. Rademacher
Courtney Manzel
DOW, LOHNES & ALBERTSON, PLLC
1200 New Hampshire Avenue, NW
Suite 800
Washington, DC 20036
(202) 776-2000

Its Attorneys

April 30, 2004