

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

In the Matter of)	
)	
Implementation of the Telecommunications Act of 1996:)	CC Docket No. 96-115
)	
Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information;)	
)	
Petition for Rulemaking to Enhance Security And Authentication Standards for Access to Customer Proprietary Network Information)	RM-11277
)	

REPLY COMMENTS OF METROPCS COMMUNICATIONS INC.

Mark A. Stachiw
Damien Falgoust
METROPCS COMMUNICATIONS, INC.
8144 Walnut Hill Lane, Suite 800
Dallas, Texas 75231
Telephone: (214)-265-2550
Facsimile: (866)-685-9618

Lynn R. Charytan
Dileep S. Srihari
WILMER CUTLER PICKERING
HALE AND DORR LLP
1875 Pennsylvania Avenue, NW
Washington, D.C. 20006
Telephone: (202)-663-6000
Facsimile: (202)-663-6363

Counsel for MetroPCS Communications Inc.

June 2, 2006

TABLE OF CONTENTS

INTRODUCTION AND SUMMARY	1
DISCUSSION	3
I. New CPNI Rules Are Unnecessary.....	3
II. The Commission Should Reject Proposals that Would Burden Carriers While Providing No or Marginal Additional CPNI Security.....	6
III. Any Rules the Commission Does Adopt Must be Broad Enough to Permit Carriers to Design Flexible Solutions to Serve Their Customers	12
CONCLUSION	22

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

In the Matter of)	
)	
Implementation of the Telecommunications Act of 1996:)	CC Docket No. 96-115
)	
Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information;)	
)	
Petition for Rulemaking to Enhance Security And Authentication Standards for Access to Customer Proprietary Network Information)	RM-11277
)	

REPLY COMMENTS OF METROPCS COMMUNICATIONS INC.

MetroPCS Communications Inc. (“MetroPCS”)¹, by its attorneys, respectfully submits these reply comments in the above-captioned proceeding.²

INTRODUCTION AND SUMMARY

As the comments in this proceeding broadly demonstrate, the imposition of new, burdensome requirements are neither necessary nor appropriate for the protection of customer proprietary network information (“CPNI”). As an initial matter, the data mining or “pretexting” issues that were the basis for this proceeding were the result of fraud and similar schemes rather than insufficient, or inadequately enforced, carrier practices. To the contrary, as the comments show, carriers are universally committed to

¹ For purposes of these Comments, the term “MetroPCS” refers to the parent company (MetroPCS Communications, Inc.) and all of its Commission licensed subsidiaries.

² Notice of Proposed Rulemaking, *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and other Customer Information*, 21 FCC Rcd. 1782 (2006) (“NPRM”).

safeguarding their customers' information and have adopted a variety of different mechanisms and procedures to do so.³ Accordingly, layering on the panoply of rules proposed in the *NPRM* would not materially advance consumer security: it merely would encumber carriers in their ability to serve their customers and impose significant costs, which would disproportionately and particularly burden smaller carriers.

Further, adoption of granular, prescriptive CPNI requirements would be seriously misguided. MetroPCS agrees with CTIA and other commenters that the Commission should, at most, adopt basic guidelines or principles that leave carriers with the flexibility to adopt particular measures that best suit their business models. The particular measures that work best for one carrier may be poorly tailored for another, based on differences in the size of the two carriers, the services they provide, the technologies they use, the rate structures of the carriers, and their billing methods — to name just a few. In addition, as MetroPCS and many other carriers showed, carriers tailor various CPNI safeguards and practices to best serve their customers' needs. Indeed, in competitive industries such as wireless, the level of privacy protection and security a carrier offers is a feature that may very well dictate success or failure in the marketplace. That market pressure is an effective means of ensuring that carriers adopt well-designed, efficient privacy measures for their customers' information — one far more likely to succeed than heavy handed, uniform rules that seek to dictate to carriers precisely what types of CPNI rules may be adopted.

³ It is critical to note that although carriers all argue that safeguarding their customer's information is important, each carrier has designed its systems so as to protect that data in a way that is most economically reasonable for that carrier. No carrier supports a one-size-fits-all approach, and none is warranted.

In short, rather than rush to issue new rules, the Commission should focus its efforts on remedying the real problem, by supporting efforts to penalize those involved in the fraud: the pretexters. The Commission's existing privacy rules already have led carriers to adopt a host of effective measures, and more rules are not likely to result in better protection. To the extent the Commission does believe additional rules are necessary, it should proceed cautiously: it should limit itself to rules that are relevant to the pretexting issues at hand, and it should adopt general principles or duties, leaving carriers with the flexibility to implement practices best suited to their business models and serve their customers efficiently. This is important for all carriers, but as the record shows, it is essential for smaller carriers like MetroPCS. Like other smaller carriers, the company would be particularly encumbered by the costs and burdens that would almost certainly be involved in the implementation of a new, detailed CPNI regime.

DISCUSSION

I. New CPNI Rules Are Unnecessary.

The fundamental message expressed by the majority of comments in this proceeding is that there is no need for a new flurry of CPNI rules and regulations. The record in this docket, press reports, and the court proceedings involving the events that precipitated this proceeding all make clear that those privacy breaches did not stem from gaps in the Commission's existing CPNI rules or lax carrier protection of consumer information, but from acts of fraud perpetrated by outsiders.⁴ Indeed, the comments

⁴ See, e.g., Comments of CTIA at 8 (“[C]arriers have not knowingly released information to anyone other than the supposed customer.”); Comments of Charter Communications, Inc. at ii (“pretexters who fraudulently obtain CPNI” are “the source of the problem”); *id.* at 1; Comments of Verizon Wireless at 2 (pretexting “succeeds by fraudulently inducing a carrier employee” to disclose CPNI).

overwhelmingly show that, like MetroPCS, providers across the board are uniformly committed to protecting consumer privacy through effective CPNI safeguards, and that they have adopted a range of different measures to do so. There is no dispute that protecting CPNI is a core obligation owed by carriers to their customers: one not only imposed by effective FCC regulations, but rightfully demanded by the public.

In fact, as MetroPCS and several other commenters noted, the degree and effectiveness of a carrier's CPNI-safeguarding measures have become a factor in attracting customers in an increasingly competitive communications marketplace. As Sprint Nextel noted, for example, "[C]ustomers concerned about security will naturally migrate to those carriers who offer the best perceived security practices, particularly in light of the publicity surrounding CPNI breaches over the past year."⁵ Or, as the National Cable and Telecommunications Association pointed out, a "disregard for the problems raised in the Notice would hardly be a sound strategy for attracting and retaining new telephone customers."⁶ Charter Communications noted that recent studies have shown that 20% of customers immediately terminate their relationship with a company after being informed that the company lost their personal information - and another 40% consider doing so.⁷ Companies suffering from security breaches have also seen a reduction in their stock price.⁸

⁵ Comments of Sprint Nextel Corporation at 11 ("Comments of Sprint Nextel").

⁶ Comments of National Cable & Telecommunications Association at 2.

⁷ See Comments of Charter Communications at 8 & n.24 (citing *Survey: Data Losses Spur Consumer Flight*, CIO today, Jan. 27, 2006, available at <http://www.cio-today.com/story.xhtml?story-id=123000030QXI>).

⁸ See *id.* at 9 & n.26.

These market-driven pressures already provide carriers with powerful incentives to provide protection for their customers' CPNI above and beyond the specific requirements of the FCC's CPNI rules, and thus make new rules unnecessary. Indeed, such incentives, which lead carriers to tailor protective measures to any specific risks posed by their service models and their customers' unique needs, are likely to be even more effective than a new round of blunt, one-size fits all government rules.

Accordingly, the Commission should proceed with caution, and not assume that "more" rules are necessarily "better." A better use of Commission *and* industry efforts would be to continue and reinforce enforcement efforts against the perpetrators of pretexting. The FTC and at least five state governments are engaged in litigation against web-based data brokers that sell call detail records, with other investigations underway.⁹ At least 17 civil lawsuits have been filed, and carriers have been successful in obtaining injunctions or restraining orders to prevent further pretexting activities.¹⁰ And Congress has committed itself, with the industry's support, to adopting stringent laws designed to expressly penalize data brokering fraud. Such efforts, which are targeted at the actual wrongdoers, are the proper government means of redressing the recent spate of privacy violations, rather than new rules aimed at the carriers that have been the victims of that activity. And carriers and providers, meanwhile, can be counted on to take private initiatives to reinforce their own internal measures — without the need for a new round of cumbersome regulatory requirements.

⁹ See Comments of Attorneys General of the Undersigned States at 2 ("Comments of NAAG"); Comments of CTIA at 7 & n.16 (noting FTC investigations).

¹⁰ See, e.g., Comments of NAAG at 2; Comments of Verizon Wireless at 5-7.

II. The Commission Should Reject Proposals that Would Burden Carriers While Providing No or Marginal Additional CPNI Security.

As CTIA and others made clear in their comments, this proceeding should not be used to create CPNI measures that have no relevance to preventing pretexting or other fraudulent access to consumer information.¹¹ The Commission should reject outright proposals that simply would layer additional obligations on providers without any corresponding benefits to consumer security and privacy in that regard.

There are many such proposals in the record. EPIC and other commenters apparently see this proceeding as an opportunity to convince the Commission that carriers should be compelled to implement every possible precaution and safeguard that can be conceived.¹² But that is a seriously overbroad response to the pretexting problem — especially given that *no* set of rules can provide a complete guarantee against such fraudulent activity. Indeed, fraud-based violations of consumer privacy occur in all industries, notwithstanding the protections in place — as is perhaps most evident in the credit card industry, which has been closely regulated in this regard for years.¹³

¹¹ *See, e.g.*, Comments of CTIA at ii (“This proceeding . . . should not be used to create CPNI procedures unrelated to the pretexting problem . . .”).

¹² *See, e.g.*, Comments of the People of the State of California Public Utilities Commission at 5 (requiring carriers to allow customers to have unlisted cell phone numbers) (“Comments of the California PUC”).

¹³ And the record here shows that data brokers typically have already violated customer privacy and obtained a host of proprietary customer information long before contacting the provider, making it almost impossible to detect or control the fraud through measures such as passwords, or requirements for date of birth, address, or other such information requirements. *See* Comments of NAAG at 3; Comments of EPIC, *et al.*, at 12 (noting that “[b]iographical information is easily obtainable by pretexters” and that “[d]ozens of websites advertise the availability of Social Security numbers, dates of birth, and mother’s maiden names”).

Accordingly, here, as in every other effort to advance the public interest, the Commission must carefully balance the costs of new rules against the benefits: rules that merely encumber service providers while not remedying the problem at hand will ultimately serve no one.

Thus, the rules adopted in this proceeding should be designed to shore up specific gaps, if any, in the Commission's existing rules, or to address specific shortcomings, if any, in carrier practices, to the extent either may have led to the data brokering problems or other security breaches. But the Commission should reject the invitation to make this proceeding a wish list of "most restrictive procedures" without regard to the costs and burdens associated with such measures. In particular, MetroPCS advocates that the Commission reject each of the following proposals as overbroad and unjustified:

Encryption. EPIC's proposal that carriers be required to encrypt customer records should be rejected. The comments confirm that requiring encryption of stored CPNI would be an expensive solution to a non-existent problem. There is no evidence from any carrier that CPNI has been compromised through "hacking" into databases.¹⁴ Even carriers such as Alltel that have voluntarily implemented some forms of encryption agree that there is no verified threat to centralized back-end databases.¹⁵

The absence of any viable problem makes the costs of implementing any type of encryption proposal all the more indefensible. One estimate places the overall cost of

¹⁴ See, e.g., Comments of AT&T Inc. at 16, Comments of BellSouth Corporation at 21; Comments of Cingular Wireless LLC at 13; Comments of Qwest Communications International Inc. to Additional Customer Proprietary Network Information Rulemaking at 10 & n.23 ("Comments of Qwest"); Comments of Sprint Nextel at 14.

¹⁵ See Comments of Alltel Corporation at 6.

implementing encryption at \$1,000 to \$2,000 per line for smaller carriers.¹⁶ The costs include not only technology but also the resources needed to re-train employees and the various other administrative expenses associated with implementing new systems.¹⁷ Furthermore, as at least one commenter points out, encryption results in slower performance.¹⁸ In light of all this, it makes no sense whatsoever to subject carriers to an encryption mandate. And such a requirement would be particularly unjustified, and burdensome, for a smaller company like MetroPCS, which has never experienced a hacking issue, and which cannot as readily absorb the high costs of implementing a new data system.¹⁹

Audit Trails. The *NPRM* sought comment on EPIC's proposal to require carriers to track all instances when an effort was made to access customer records, whether information was disclosed, and to whom;²⁰ NASUCA proposed in its comments that

¹⁶ See Comments of OPASTCO at 5.

¹⁷ See, e.g., Comments of BellSouth Corporation at 22 (“millions of dollars would be needed simply to complete initial planning and analysis for additional encryption initiatives”).

¹⁸ Comments of Charter Communications at 29 (quoting Ray Wagner, Research Director for Information Security Strategies, Gartner).

¹⁹ Furthermore, if the Commission decides to go down this path, it will need to decide what form of encryption is necessary or appropriate. As the Commission knows, there are many levels of encryption and without any real showing that hacking is occurring, determining the level of encryption will be at best a guess. Further, encryption only deals with the carrier's systems and not with on-line systems that may be used by customers to access their data. All of this suggests that in the absence of a specific need, the Commission should not go down this road.

²⁰ See *NPRM* at 1789 ¶ 17 (citing Petition of the Electronic Privacy Information Center for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information, filed in Docket No. 96-115, Aug. 30, 2005, at 11 (“EPIC Petition”).

carriers be required to establish audit trails that identify (1) when a customer has contacted the carrier, (2) how the customer verified his or her identity, (3) whether CPNI was requested, and (4) whether and what CPNI was disclosed.²¹ Though MetroPCS does track requests for call records (which it can easily do given the small number of such requests that it receives), there is no justification for imposing this practice as a mandate — especially one that includes the various details contained in the EPIC and NASUCA proposals.

To begin with, as the comments make clear, audit trails, while possibly helpful in tracking CPNI breaches, do not actually *prevent* them.²² Given this, there is no basis to impose on carriers the enormous costs of an extensive audit requirement such as EPIC or NASUCA propose. In fact, as many commenters pointed out,²³ the Commission rejected an audit trail requirement in 1999, precisely because the excessive burdens involved could not be justified.²⁴ These costs are likely to be at least as high today, if not higher;

²¹ See Comments of NASUCA at 11.

²² See, e.g., Comments of Qwest at 12 (“For example, an audit trail system that tracks each and every question asked by a customer service representative during the course of an inbound call would not solve the social engineering problem. If a pretexter knows the answers to the questions, the audit trail indicates only that the correct answers were provided.”).

²³ See, e.g., Comments of BellSouth Corporation at 18-19; Comments of Global Crossing North America, Inc., at 4; Comments of Sprint Nextel at 12.

²⁴ See Order on Reconsideration and Petitions for Forbearance, *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, 14 FCC Rcd 14409, 14475 ¶ 127 (1999) (An “electronic audit trail requirement would generate ‘massive’ data storage requirements at great cost. As it is already incumbent upon all carriers to ensure that CPNI is not misused and that our rules regarding the use of CPNI are not violated we conclude, on balance, such a potentially costly and burdensome rule does not justify its benefit.”).

indeed, the data storage requirements alone would be excessive. And the costs of this “monumental and very expensive undertaking” could be particularly prohibitive for smaller carriers.²⁵ For example, one estimate placed the costs of the “extensive re-design” of software applications to properly detect and log any access to consumer data at \$2,000 to \$3,000 per access line for small rural carriers.²⁶ Thus, to the extent the Commission adopts any audit rule at all, it must scale the requirement back, and provide significant flexibility with respect to record keeping and systems, especially for smaller carriers.

Limits on Data Retention. There is broad consensus that EPIC’s proposal to require deletion of call records when no longer needed for billing or dispute purposes²⁷ — or NASUCA’s proposed 18-month maximum record retention period²⁸ — would produce no benefits in combating pretexting.²⁹ Nothing in the record suggests that older records are particularly vulnerable, nor is there any reason to believe that data miners are particularly (or at all) interested in such records.³⁰ And some carriers, like MetroPCS,

²⁵ Comments of Dobson Communications at 7.

²⁶ See Comments of OPASTCO at 4.

²⁷ See NPRM at 1790 ¶ 20 (citing EPIC Petition at 11).

²⁸ See Comments of NASUCA at 22-23.

²⁹ See, e.g., Comments of AT&T Inc. at 16; Comments of Cingular Wireless LLC at 24; Comments of Qwest at 16-17 (limiting data retention “fails to resolve the problem the Commission is trying to address - data brokers fraudulently securing current customer records from carriers”).

³⁰ See Comments of the Public Service Commission of the State of Missouri at 4 (“[O]lder CPNI . . . may be of little commercial use to those who obtain it improperly or illegally. It is a consumer’s current information that is sought by entities improperly using the data.”). To be sure, there is some logic to the argument that carriers have no

already retire older records (while not destroying them), so that requests for older data will already raise additional scrutiny and be *less* susceptible to fraud.³¹ At the same time, carriers and regulators alike express significant concern that rules requiring destruction of older data could actually harm consumers: the Ohio Public Utilities Commission, for example, opposes a destruction requirement because it contends that such a rule would make it harder for carriers to respond to legitimate consumer inquiries.³² Meanwhile, the Departments of Justice and Homeland Security argue that any requirement that carriers destroy older records could adversely affect law enforcement efforts.³³

Special Rules for Wireless Carriers. MetroPCS also opposes the suggestion by the National Association of Attorneys General (“NAAG”) that the Commission adopt unique, additional rules for wireless carriers because they may have access to location

legitimate need to retain records when those records are no longer needed for dispute or billing purposes. But as BellSouth points out, there is no way to convert this principle into a rule of general applicability. *See* Comments of BellSouth Corporation at 23. The only rule that the Commission could even consider adopting would be the general principle that carriers keep records no longer than necessary, a practice that may naturally be adopted by carriers even without any such rule, given limited data retention capabilities. Further, that length of time will differ in different states: in many instances, laws require companies to keep records for longer rather than shorter periods of time. Some jurisdictions make destruction of records a crime under certain circumstances. All of this militates against adopting broad based destruction rules.

³¹ *See* Comments of MetroPCS at 11 (noting that call records are archived after six months, and MetroPCS does not regularly access or release this older data); Comments of Verizon Wireless at 17 (noting that its customer service representatives do not have access to the type of old information that would be purged under the EPIC proposal).

³² *See* Comments of Public Utilities Commission of Ohio at 15.

³³ *See* Comments of the United States Departments of Justice and Homeland Security at 6-7.

information.³⁴ Wireless carriers are already subject to special restrictions on their use of and duty to protect location information: As NAAG itself points out, in 2002, the FCC found that Section 222(f) of the Communications Act provides clear protections for consumers and legal obligations for providers.³⁵ While NAAG argues that such information would be of great value to advertisers, stalkers, and debt collectors,³⁶ there is no evidence in the record that data brokers or others have obtained improper access to location information, or that there has been improper release or use of such information by wireless carriers. This proceeding should not be used as an opportunity to simply “pile on” in the absence of an identified harm.

III. Any Rules the Commission Does Adopt Must be Broad Enough to Permit Carriers to Design Flexible Solutions to Serve Their Customers.

Any rules the Commission *does* adopt must be designed to give carriers the flexibility to serve their customers. The one-size-fits-all, prescriptive measures proposed by EPIC and NASUCA, and supported by some commenters, would unduly interfere with the carrier-customer relationship and would impose significant costs on carriers (especially smaller ones) without producing any countervailing benefit. Thus, to the extent new rules are necessary, they should be broad guidelines that provide carriers with room to tailor their own specific practices and rules. The Commission should eschew rules that unduly restrict carriers’ choices or that are not remotely tailored to address demonstrated risks or harm.

³⁴ See Comments of NAAG at 12-13.

³⁵ See *id.* at 13.

³⁶ See *id.* at 12.

As MetroPCS and many other commenters showed, carriers of different types and sizes already have adopted a host of different measures to safeguard CPNI today, which, despite their differences, have proved effective. These carrier-specific measures tend to reflect distinctions in the carriers' size, business models, or customer types, as well as individual carrier's experience with the risks and benefits of different approaches, and the best balance between their customers' desire for efficiency and privacy.

MetroPCS, for example, has a pre-paid business model that eliminates the need for paper billing and significantly reduces the number of call records produced *or* requested; in fact, MetroPCS receives fewer than 400 requests for detailed billing records annually,³⁷ and less than 1% of its customers order a monthly record of their calls.³⁸ This makes it easier for MetroPCS to track and handle CPNI requests, allows it to adopt certain procedures that might be burdensome for some carriers (like emailed CPNI request confirmation notices), and makes some measures (computerized "audit" trails and text-message verification of CPNI requests to customers' phones) unnecessary.

In contrast, larger carriers like Verizon Wireless — especially larger carriers offering per-minute billing plans — may release CPNI in response to customer calls or billing inquiries "millions of times each month."³⁹ Carriers with this type of volume face different challenges and must adopt different measures. For example, such carriers likely do not have the luxury of elevating each request for CPNI to a supervisor, as MetroPCS

³⁷ See Comments of MetroPCS at 3.

³⁸ See *id.* at 4.

³⁹ See Comments of Verizon Wireless at 16-17.

does. Nor might such carriers meet with success in requiring verification of CPNI requests by sending a text message to a customer's phone.

In other words, differences in carriers' CPNI practices may reflect careful efforts by carriers to best tailor their practices to the realities of particular companies — efforts that should be encouraged by the Commission rather than suppressed in favor of uniform rules that eliminate carrier discretion to shape measures that work best for their company and customers. The Commission's existing rules allow this, and MetroPCS continues to believe that those rules have generally been effective and sufficient and that no more rules are required. Nevertheless, like many other commenters, MetroPCS would not object to the adoption of additional core principles or duties, such as a requirement that carriers put in place measures to verify customer identity, avoid releasing certain sensitive data on incoming calls, or publicize their privacy and security policies. It is critical, however, that the Commission reject the invitation to mandate a prescriptive, "one-size-fits-all" framework that dictates *how* carriers comply with those principles or duties. That sort of micromanagement is not necessary to safeguard CPNI, and ultimately would be less successful than customer-driven, company specific procedures and policies. And to the extent the Commission seeks to provide more detailed guidance, MetroPCS agrees with the many commenters that made clear that such specific rules should serve solely as a "voluntary" safe harbor,⁴⁰ while leaving carriers free to fashion other measures that may be equally or more effective, and better tailored to their needs.

⁴⁰ See, e.g., Comments of Cingular Wireless LLC at 31-33; Comments of Qwest at 34-36; Comments of Verizon Wireless at 20-21.

With that introduction, MetroPCS addresses several of the proposals in this proceeding:

Identify Verification. Several commenters have proposed that the Commission require that carriers adopt strict customer verification measures to ensure that CPNI is released only to its owner.⁴¹ MetroPCS does not oppose a general rule that carriers take reasonable measures to verify the identity of a customer before releasing his or her CPNI; in fact, the company already requires that customers set and use passwords to access CPNI.⁴² However, the Commission should not dictate the specific means carriers must employ for verification. For example, even though MetroPCS has used passwords in connection with CPNI access very successfully, the company opposes any rule that would mandate the use of passwords (or passwords of any particular type or make-up). For one thing, a password rule would inevitably result in even more granular requirements, such as rules governing lost passwords, password changes, length of passwords, formulating passwords, and the like: issues that would embroil the Commission in the minute details of the carrier-customer relationship. In addition, the comments suggest that many carriers have had negative experiences using passwords. Some commenters noted that password requirements can have a negative effect on a customer's service experience, because lost passwords, and the need to reset them, are

⁴¹ See, e.g., Comments of EPIC, *et al.*, at 13 (proposing "shared secrets" as an improvement on passwords); Comments of NAAG at 15-16 (proposing that lost passwords be mailed or emailed only to the applicable address on file).

⁴² See Comments of MetroPCS at 6-7.

seen as a significant inconvenience.⁴³ Commenters also argued that customers appear not to want passwords, noting that even when that option was available, many customers declined to set passwords.⁴⁴ Perhaps in response to such concerns, some commenters have suggested that the Commission simply adopt a password *option*⁴⁵ — a requirement with which MetroPCS obviously already complies. But it is not clear that even this requirement is justified, except perhaps as a safe harbor: carriers that do not already have a password option have reported that adding such a requirement could cost several hundred thousand dollars⁴⁶ — a cost that the Commission must take into account in determining whether a password rule is appropriate.⁴⁷

That is especially the case given that there is no evidence that the use of passwords has prevented pretexting. Indeed, password change mechanisms, which must be offered if customers are using passwords, may make passwords no more effective than

⁴³ *See, e.g.*, Comments of AT&T Inc. at 9-10; Comments of Qwest at 21-22. Indeed, if passwords are made more obscure in order to increase their effectiveness, customers will become frustrated and fewer will use the password option. To be useful, passwords need to be easily remembered.

⁴⁴ *See, e.g.*, Comments of AT&T Inc. at 9; Comments of BellSouth at 16; Comments of Charter Communications at 25-26; Comments of Cingular Wireless LLC at 19-20; Comments of Qwest at 21.

⁴⁵ *See, e.g.*, Comments of CTIA at 13 (supporting a password option requirement); Comments of Verizon Wireless at 21 (supporting a password option requirement as part of a “safe harbor” provision).

⁴⁶ *See* Joint Comments of Eschelon Telecom, Inc., *et al.*, at 6.

⁴⁷ Further, even in adopting a rule that carriers must offer an option, the Commission would inevitably be drawn into having to define the details of a minimally acceptable “option” — ultimately dictating the specifics of carrier password procedures.

EPIC's "shared secret" concept⁴⁸ or other approaches that carriers may use. Thus, forcing providers to revamp their systems to use a particular mechanism may impose expense that produces marginal or no benefit as compared to the provider's existing practice. In short, effective verification measures are important, but the Commission should not impose a specific set of verification requirements.

Privacy Policy. Some commenters have suggested that that the Commission impose a general duty on carriers to disclose their privacy practices and security measures.⁴⁹ MetroPCS agrees that this is a reasonable requirement, provided that the Commission steer clear of dictating the details or form of that disclosure. Carrier disclosures to customers are a basic component of the carrier-customer relationship, and both the form and content of such disclosures do (and should) reflect the specifics of that relationship.

For example, the Pennsylvania PUC's suggestion that the Commission require bill inserts⁵⁰ assumes that all carriers routinely provide paper bills, but as MetroPCS explained in its opening comments, the company does not routinely do so because it does not routinely bill its customers with paper bills.⁵¹ Instead, the company posts its subscriber policy notice on its website, which is consistent with its primarily paper-free

⁴⁸ See Comments of EPIC, *et al.*, at 13. As NASUCA explained in its comments, "The inherent problem with most 'shared secret' systems is that the security questions used cover matters that can be tracked down fairly easily using available public records." Comments of NASUCA at 17.

⁴⁹ See Comments of CTIA at ii; Comments of Verizon Wireless at 18-19.

⁵⁰ See, *e.g.*, Comments of Pennsylvania Public Utility Commission at 6.

⁵¹ See Comments of MetroPCS at 4 (customers typically receive a text message on their phone reflecting the bill for the next month).

business model and with its customers' expectations. Given that this approach and others are effective means of providing notice, it would be senseless to interfere with that business model by compelling the company to provide a mailing to all its customers, a requirement that would impose significant additional costs on MetroPCS.

Filing of Annual CPNI Certification. Many commenters, including CTIA and others, support the Commission's tentative conclusion that carriers be required to file their annual CPNI certification with the Commission, and propose that the certification represent that the carrier has implemented security measure to prevent unauthorized CPNI disclosure and has trained its personnel in CPNI privacy and security measures.⁵² MetroPCS supports such a requirement, so long as the Commission does not require the listing of all consumer complaints regarding CPNI disclosure or all action taken against data brokers.⁵³ As CTIA makes clear, this requirement is burdensome, and vague, and the information will be of limited utility: it certainly will not aid in *preventing* pretexting.⁵⁴

Customer Notification. EPIC and others have proposed that the Commission require carriers to notify customers whenever CPNI is requested. MetroPCS does so, by emailing the customer each time a request for the customer's CPNI is received, but the record makes clear that larger carriers that serve more customers and receive more such

⁵² See, e.g., Comments of CTIA at 9; Comments of Qwest at 35-36; Comments of Verizon Wireless at 19.

⁵³ See *NPRM* at 1793 ¶ 29.

⁵⁴ See Comments of CTIA at 9-11.

requests would find this requirement excessively burdensome.⁵⁵ MetroPCS does not believe that a notification mandate is necessary if effective verification is required, but if the Commission *were* to adopt a general rule requiring notification as an extra layer of protection, it should allow carriers to notify their customers however they see fit: the Commission should not require email versus telephonic notification, for example.

Some commenters also propose that the Commission adopt a rule requiring notification in the event of a serious security breach.⁵⁶ It is not clear how this rule helps *prevent* fraudulent CPNI access, since it would be triggered only after the fact.⁵⁷ Nevertheless, such a requirement would not be unreasonable or seriously costly, provided that the Commission does not require reporting of *potential* breaches or suspicious conduct.⁵⁸ Moreover, the Commission should steer clear of specifying the details

⁵⁵ See, e.g., Comments of AT&T Inc. at 13-14 (describing “significant additional costs that would ultimately be passed on to consumers”); Comments of Cingular Wireless LLC at 29 (describing “tremendous” negative financial impact) Comments of Qwest at 19; Comments of Sprint Nextel Corporation at 16 (additional notice regime would be “extremely expensive”).

⁵⁶ See, e.g., Comments of Charter Communications at 35; Comments of Public Utilities Commission of Ohio at 11.

⁵⁷ DOJ and DHS propose that carriers notify law enforcement prior to victim notification, with law enforcement having the ability to request a reasonable delay in customer notification if notification might harm related law enforcement investigative efforts. See Comments of the United States Departments of Justice and Homeland Security at 13-15. While there are obvious law enforcement benefits to such a rule, it, too does not help in preventing pretexting, but instead addresses other law enforcement issues. Further, such a requirement might be very unattractive to customers, who may need to know quickly that their private data has been released in order to prevent against identity theft and the like. Such a rule should be adopted only if carriers are simultaneously insulated from any liability for complying.

⁵⁸ The *NPRM* suggestion that carriers be required to notify customers every time security “*may* have been breached,” *NPRM* at 1791 ¶ 21 (emphasis added), is significantly

concerning the timing and method of notification: as with routine notifications, carriers should be free to use the method that best suits their business and customer group.⁵⁹

Once a CPNI request has been verified, NAAG proposes that the Commission require carriers to only transmit call records in hard copy to the billing address listed on the account, or by emailing the records only after the customer responds in the affirmative to a text message.⁶⁰ NAAG also proposes that the Commission require every customer to show photo identification when trying to obtain call records from a carrier's store.⁶¹ Here again, however, the Commission should avoid any rule other than a very general requirement, since carriers follow different practices in transmitting call records to customers after a legitimate request has been made. MetroPCS, for example, will transmit call records to any address after a request has been verified. On the other hand, some carriers transmit billing records only to the billing address on file,⁶² and/or have a specific prohibition on transmitting records by email.⁶³ Some carriers allow access to records at a store location after presenting a photo ID, or through a password-protected

overbroad and would result in needlessly upsetting customers. Such a requirement could be read so as to require thousands of notifications for routine events that are not in fact problematic. *See* Comments of Charter Communications at 38.

⁵⁹ Indeed, one commenter noted that some smaller carriers might even find it more economical to call customers. *See* National Telecommunications Cooperative Association Initial Comments at 4.

⁶⁰ *See* Comments of NAAG at 14-15.

⁶¹ *See id.* at 16.

⁶² *See, e.g.,* Comments of Dobson Communications at 5; Comments of Eschelon at 4; Comments of Texas Statewide Telephone Cooperative at 2 (call records only mailed to billing address, unless another person has been previously authorized to receive CPNI).

⁶³ *See* Comments of Dobson Communications at 5.

website.⁶⁴ There may be good reasons that different carriers prefer different practices. Since MetroPCS has an email-driven practice, for example, it would be incongruous and potentially cost prohibitive to require it to provide only written records; further, because MetroPCS may serve a population of people that move frequently and yet may not regularly update their physical address (because of MetroPCS' s paperless model), it would make little sense to restrict MetroPCS to sending records only to the physical "address on file." Indeed, for MetroPCS in particular, an e-mail address is a preferable and likely more successful means of reaching the customer. On the other hand, a carrier that never communicates with its customers by email might be particularly uncomfortable being required to send such records to an email address. Unless one of these practices has been shown to lead to unique security breaches, the Commission should avoid dictating this element of a carrier' s relationship with its customer.

Disclosure of Personal Information on Inbound Calls. CTIA supports a rule prohibiting a carrier from disclosing a customer' s social security number, taxpayer identification number, credit card number, or billing name and address in response to inbound customer calls.⁶⁵ MetroPCS does not oppose this basic restriction, as long as companies are given time to train their employees and institute proper measures. Any such rule must leave companies with the flexibility to disclose such information as necessary from the carrier' s offices to retail store employees or field personnel, however.

⁶⁴ See, e.g., Comments of Qwest at 33, 34.

⁶⁵ See Comments of CTIA at 3.

CONCLUSION

For the foregoing reasons, MetroPCS urges the Commission to reject the EPIC proposals, and at most, to adopt the broad general rules set forth here. Further, the Commission should, in adopting any rules, be particularly sensitive to the burdens and costs imposed on smaller carriers. While Cingular suggests that all carrier's data and the obligations they owe to consumers are equal,⁶⁶ requirements and measures that might be reasonable when applied to a larger carrier with more resources may have a disproportionately costly and burdensome impact on smaller carriers. And fewer customers may mean that smaller carriers face a lesser risk of fraudulent CPNI access. Thus, as several commenters argued,⁶⁷ the Commission should at a minimum provide smaller carriers with more flexibility and/or a gradual phase-in of any new requirements.

Respectfully Submitted,

MetroPCS Communications, Inc.

/s/ Lynn R. Charytan

Lynn R. Charytan
Dileep S. Srihari
WILMER CUTLER PICKERING HALE AND DORR LLP
1875 Pennsylvania Avenue, NW
Washington, D.C. 20006
Telephone: (202)-663-6000
Facsimile: (202)-663-6363

⁶⁶ See Comments of Cingular Wireless LLC at 33.

⁶⁷ See, e.g., Comments of Alexicon Telecommunications Consulting at 7-8; Comments of the Independent Carrier Group at 6; Comments of National Telecommunications Cooperative Association at 3.

Mark A. Stachiw
Senior Vice President, General Counsel and Secretary
Damien Falgoust
Corporate Counsel and Assistant Secretary
METROPCS COMMUNICATIONS, INC.
8144 Walnut Hill Lane, Suite 800
Dallas, Texas 75231
Telephone: (214)-265-2550
Facsimile: (866)-685-9618

Its Attorneys

June 2, 2006