April 9, 2003

Joel H. Peck, Clerk
Document Control Center
State Corporation Commission
1300 East Main Street
Richmond, VA 23219

Ex Parte: Establishment of a Performance Assurance Plan for
Verizon Virginia Inc.

Case No. PUC-2001-00226

Dear Mr. Peck,

Enclosed for filing with the Commission are an original and fifteen copies of the Comments of AT&T Communications of Virginia, LLC to the Petition of Verizon Virginia Inc. for a Waiver of Certain Service Quality Results Measured Under the Performance Assurance Plan for January 2003.

Thank you for your attention to this matter.

Sincerely,

Mark A. Keffer

CC: Service List

COMMONWEALTH OF VIRGINIA
STATE CORPORATION COMMISSION
AT RICHMOND

Commonwealth of Virginia, ex rel. State Corporation Commission	:	**Case No. PUC-2001-00226**
Ex Parte: Establishment of a Performance Assurance Plan for Verizon Virginia, Inc.	:	

COMMENTS OF AT&T COMMUNICATIONS OF VIRGINIA, LLC TO THE PETITION OF VERIZON VIRGINIA, INC. FOR A WAIVER OF CERTAIN SERVICE QUALITY RESULTS MEASURED UNDER THE PERFORMANCE ASSURANCE PLAN FOR JANUARY 2003

AT&T Communications of Virginia, LLC ("AT&T") opposes Verizon Virginia, Inc.'s ("Verizon's") March 17, 2003 Petition for a Waiver of Certain Service Quality Results for January 2003 as Measured Under the Performance Assurance Plan ("Petition"). As AT&T will explain in detail below, Verizon has failed to make even a *prima facie* case that the so-called "Slammer Worm" computer virus was an "emergency, catastrophe, [or] natural disaster" beyond its control that would excuse Verizon from its wholesale performance obligations under the Performance Assurance Plan ("PAP"). Thus, the State Corporation Commission ("Commission") should not permit Verizon to evade its important responsibilities under the PAP to provide adequate service to its CLEC wholesale customers, and the payment of $886,819 in bill credits to CLECs for its failure to provide such service as a direct result of an event that was eminently preventable through reasonable action.

I. Statement of Position

As its name suggests, the Performance Assurance Plan ("PAP") is intended to assure that Verizon will provide high-quality performance to its wholesale customers. This is accomplished

by, among other things, confronting Verizon with cost consequences for poor service performance.

The PAP was not adopted in a vacuum. When Verizon sought authority to enter the long-distance market in Virginia, Verizon made several commitments, including giving assurance that it would provide reliable service to its wholesale customers which, in turn, compete with Verizon for local service customers. The PAP was specifically designed to confront Verizon with sufficiently meaningful penalties that it would not allow its performance to degrade – and to give affected wholesale customers meaningful compensation in the event such service degradations occurred. Thus, the object of the PAP was to ensure that Verizon would proactively meet, if not exceed, prescribed threshold performance levels.

The PAP permits waivers in certain extraordinary circumstances in which forces beyond Verizon's control result in service falling below minimum thresholds. However, the waiver provision is strict, both in terms of the truly exceptional events required to be shown and the demanding standard of proof of those events that Verizon must satisfy. Verizon must demonstrate events that are of an "extraordinary nature," that are "beyond Verizon's control," and that could not be prevented by Verizon's "normal, reasonable preparations for difficult situations." PAP at 23. Verizon must prove the extraordinary nature of the event "clearly and convincingly"— an exceptionally high standard of proof. *Id.*

Verizon asserts that an event of January 25, 2003 affecting its computer systems constituted such an event and justifies a waiver. AT&T disagrees. As AT&T demonstrates herein, Verizon's conduct with respect to addressing the known hazard to its software system was at the very least negligent. Given the criticality of the systems, and the potential costs to Verizon's customers of a successful attack, Verizon's failure to address the problem over the

course of four to six months of repeated warnings is unpardonable. Verizon's Petition comes nowhere near meeting the rightly strict set of requirements for waiver relief under the PAP.

Further, it is troubling that Verizon would use the occasion of the harm that occurred to its customers because of Verizon's negligence to attempt to avoid the consequences of a "self-enforcing" regulatory scheme that Verizon solemnly accepted to demonstrate that it would not slacken its performance with respect to wholesale customers if it gained authority to enter the retail long-distance market in Virginia. Under the circumstances, the Commission should insist that the penalties for poor performance fully apply. Otherwise, a precedent would be established in which Verizon could punish its wholesale customers twice, first through negligence or indifference and a second time through a claim that the consequences of its inaction were "beyond its control" and therefore constitute grounds for avoiding its performance commitments.

II. Verizon Was Reckless In Its Failure To Timely And Effectively Act Upon Microsoft's Repeated Warnings Regarding The "Critical" Risk That The Slammer Worm Posed To The Very System Platforms That Verizon Employs.

According to Verizon, during the weekend of January 25, 2003, certain computer systems operated by Verizon and its affiliated companies were infected by an Internet computer virus known as "the Slammer Worm." (Petition at 3-4.) Verizon further states that the virus exploited the vulnerabilities of the Microsoft SQL Server 2000 and propagated such high volumes of traffic within Verizon's system that Verizon was unable to satisfy its three pre-order wholesale measures, specifically, those set forth in PAP PO-2-02. (Petition at 3) After describing the remedial efforts it made after learning of the infection (Petition at 4-6), Verizon then contends that Verizon could not be reasonably expected to have taken timely preventative measures to inoculate its systems from the Slammer Worm. (Petition at 6-8.)

Verizon's contentions that it could not have anticipated and timely inoculated it systems against the Slammer Worm virus are without merit. The facts demonstrate that the software maker, Microsoft, had issued repeated warnings for months regarding this virus. The warnings explicitly ranked the security risk to the systems used by Verizon as "critical." The users of such systems were warned to "immediately" inoculate their systems against the Slammer Worm. Verizon took no action for months. Only after the virus struck did Verizon finally take action.

Verizon has a substantial investment in its computer systems. Prudence dictates that it would have well-trained information technology (IT) managers and that these managers would be alert to viruses such as the Slammer Worm, which, as Verizon notes, attacks "a security vulnerability in MS [Microsoft] SQL Server 2000 and MSDE 2000." (Petition at 8.) The Slammer Worm was widely known to the IT community well before January 2003. There is no reasonable basis upon which Verizon may contend that it could not have known of the virus – and the severity of the risk it posed – and effectively inoculated its system well before the virus actually reached it.

Microsoft proactively solicits information on vulnerabilities in its software, and regularly notifies users, including IT professionals, of potential vulnerabilities through what are known as Security Bulletins. In accordance with its practice, on July 24, 2002 – six full months before the Slammer Worm attack – Microsoft issued Security Bulletin MS02-039 addressed administrators of the very systems described by Verizon. The Bulletin stated:

> **Summary**
>
> **Who should read this bulletin:** System administrators using Microsoft® SQL Server™ 2000 and Microsoft Desktop Engine 2000.
>
> **Impact of vulnerability:** Three vulnerabilities, the most serious of which could enable an attacker to gain control over an affected server.

Maximum Severity Rating: Critical
Recommendation: System administrators should install the patch *immediately*.[1]

On October 2, 2002, Microsoft issued a second warning to administrators of systems using the SQL Server and MSDE 2000, Security Bulletin MS02-056. This Bulletin again noted that the Maximum Severity Rating was "Critical" and recommended that the system administrators "apply the patch to affected systems."[2]

On October 16, 2002, a third separate warning was issued, Microsoft Security Bulletin MS02-061. The Bulletin, which was directed to the system administrators of SQL Server 2000 and MSDE 2000 and two other systems, noted that the patch was for the "Slammer" worm virus that specifically affected only SQL Server 2000 and MSDE 2000. The updated version of the Bulletin MS02-061, dated February 28, 2003, notes that the original (July 2002) patch "was fully effective in eliminating the security vulnerability" but that under some circumstances, the patch was found to interfere with SQL server operations. Accordingly, "on October 30, 2002, an additional non-security hotfix (317748) was required to ensure normal operations of SQL Server."[3]

---

[1] Security Bulletin MS02-039 (Italicized emphasis added). The Bulletin, as updated on January 31, 2003, may be found at http://www.Microsoft.com/technet/security/bulletin/MS02-039.asp. A copy of same appears as Attachment A.

[2] Security Bulletin MS02-056. This Bulletin, as updated on January 31, 2003, may be found at http://www.Microsoft.com/technet/security/bulletin/MS02-056.asp. A copy of same appears as Attachment B.

[3] Security Bulletin MS02-061. This Bulletin, as updated on February 28, 2003, may be found at http://www.Microsoft.com/technet/security/bulletin/MS02-061.asp. A copy of same appears as Attachment C.

Recognizing that not all vulnerabilities have an equal impact on all customers, Microsoft uses a four-part rating system for security threats, namely, "low," "moderate," "important," and "critical." Threats assigned a "Critical" rating are deemed the most serious, precisely because the vulnerability "could allow the propagation of an Internet worm without user action." In particular, Microsoft states: "We believe that customers that use an affected product should almost always apply patches that address vulnerabilities rated 'critical' or 'important.' Patches rated 'critical' should be applied in an especially timely manner."[4] The three Microsoft Bulletins, taken together, show that warnings of a "Critical" risk to SQL Server 2000 and MSDE 2000 systems were given, "patches" were available, and that any potential "side effects" associated with the patch-inoculations had been fully resolved by the end of October 2002.

In view of Verizon's investment in its computer systems, the critical importance of those systems to Verizon's duty to fulfill its responsibilities to its retail and wholesale customers, and the gravity of Microsoft's repeated warnings, Verizon's suggestion that it did want to "rush" to implement a patch (Petition at 7) is untenable. Verizon simply chose not to familiarize itself with Microsoft's warnings[5] or, if it did, simply chose not to take the warnings seriously. Either way, Verizon's cavalier approach to its security responsibilities was not consistent with its

---

[4] http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/policy/rating.asp.

[5] Keeping abreast of new security threats is by no means difficult. Microsoft offers a free e-mail automatic notification service. "This is a free e-mail notification service that Microsoft uses to send information to subscribers about the security of Microsoft products. [¶] The goal of this service is to provide accurate information to our customers that they can use to inform and protect themselves from malicious attacks." http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/notify.asp

obligation to protect its customers from the consequences of known threats specifically aimed at the security and reliability of its systems.

The Commission should reject Verizon's contention that the Slammer Worm struck Verizon's systems "without warning." (Petition at 10) Verizon's assertion is true only in the narrowest sense that Verizon could not have predicted the exact *moment* that the virus would reach its systems. Verizon's assertion is false, however, if the implication is that Verizon was not amply and repeatedly warned of this specific threat to the very system platforms that Verizon employs. Verizon was clearly on notice – *for six months* before the Slammer Worm attack -- of the "critical" threat posed by the Slammer Worm virus to the specific software platform that its employs.

Verizon contends that it should not be held culpable for the results of the Slammer Worm attack – in other words, it should be immunized from the financial consequences of failing to perform in January 2003. Yet, Verizon failed to heed and act upon the July 2002 warning, which included a patch that fully closed the security vulnerability. Further, by October 2002, it was a matter of public information that a revised patch was availability that both closed the security vulnerability and caused no operational difficulties. Since Verizon recklessly disregarded these announcements and remedies, Verizon is not entitled to a waiver under the PAP.

III. Exonerating Verizon From The Financial Consequences Under The PAP Of Its Own Negligence Would Establish A Precedent Whereby Verizon Could Degrade Wholesale Performance And Evade Its PAP Commitments.

When the Slammer Worm finally attacked the software systems that Verizon left exposed, one consequence was a degradation of certain services, the performance of which is measured under the PAP. Verizon's attempt invoke the *force majeure* provisions of the PAP to evade its responsibilities under the PAP for the poor service is of considerable concern since it

suggests that Verizon is seeking to establish a precedent that would undermine the effectiveness of the PAP. As AT&T noted above, the PAP was adopted as part of key public policy compact, in which Verizon could enter the competitive long-distance market in return for meaningful assurances that it would responsibly and timely provide the monopoly network facilities upon which its wholesale customers depend.

The very filing of the Petition raises a question as to whether Verizon is truly committed to the performance requirements in the PAP. The PAP was purposefully designed with self-executing bill-credit remedies intended to ensure that Verizon did not indulge a natural inclination to "backslide" once it received the interexchange relief for which it fought so ferociously. In extremely limited circumstances, the PAP's strictures may be relaxed so that Verizon will not be penalized unfairly in circumstances where equity demands forbearance or waiver. But this is not the case here.

Indeed, Verizon's Petition does not even make out a *prima facie* case to waive certain service performance results that would reduce the amount of bill credits due to competitive local exchange carriers ("CLECs"). Accordingly, on that basis alone the Commission should deny Verizon's Petition.[6]

The bill-credit remedies under the PAP are crucial to the development and protection of effective competition in the local exchange marketplace. These remedies were designed to be, and remain, a principal means of disciplining Verizon's offer and provision of vital Operations

---

[6] PAP at 23 ("Insufficient filings may be dismissed for failure to make a prima facie showing that relief is justified").

Support System ("OSS") functions to CLECs seeking to enter and compete in the local market. Because performance of such OSS functions is so important to the development of local exchange competition, and thus to the public interest, CLECs are, under the terms of the PAP, entitled to and assured of substantial bill credits when Method-of-Entry Measures and Critical Measures are not met by Verizon. These bill-credit remedies have been triggered in the instant case. There is no dispute here that Verizon failed to meet Method-of-Entry Measures for both UNEs and for Resale, and failed to meet a Critical Measure for OSS Interface Availability.[7] According to Verizon, its liability under the PAP for the month of January 2003 is $1,011,418. However, if its March 17, 2003, petition is successful, that amount will be reduced by $886,819, or nearly 88%, to $124,500. (Petition at 2.) Verizon should be required to provide the full amount of credits.

The only basis offered by Verizon for avoiding these bill credits to CLECs is a waiver provision of the PAP that is wholly inapplicable. PAP at 22-23.[8] The waiver provision relied upon by Verizon is, for good reason, exceedingly strict, both in terms of the truly exceptional events required to be shown and the demanding standard of proof of those events that Verizon must satisfy.

The PAP contemplates the possibility of a reduction of owed bill credits for vital OSS functions only where Verizon shows events that are of an "extraordinary nature," that are "beyond Verizon's control," and that could not be prevented by Verizon's "normal, reasonable

---

[7] The Commission should recognize that it cannot determine the parity effects of Verizon's actions here (on, for example, pre-ordering availability) because a direct Verizon retail analogue does not exist (since Verizon does not access pre-order information through an interface as do CLECs).

preparations for difficult situations." PAP at 23. Further, Verizon is required to prove the extraordinary nature of the event "clearly and convincingly"— an exceptionally high standard of proof.[9] *Id.* Verizon's Petition comes nowhere near meeting this rightly strict set of requirements for waiver relief.

To the contrary, Verizon makes no real attempt to show any of the elements required for a waiver. The event that Verizon claims was "beyond its control" is its simple failure to deploy an available software patch either because detection of the threat or implementation of the remedy would have required too much effort. When one takes into account all of the circumstances, including Verizon's critical obligation to provide adequate and parity service to CLECs under the PAP, Verizon's claims that it "acted in a prudent, reasonable manner" (Petition at 11) are simply not credible.

Verizon makes broad and generally unsubstantiated claims about the experience of other companies with the Slammer Worm. These claims, even if substantiated, are irrelevant to the waiver provision of the PAP, which is directed toward events that are truly exceptional and beyond Verizon's control. Thus, it is no excuse that, even if true, "[m]any other well-respected and well-run companies were also infected by the Slammer Worm and Verizon's experience

---

(Footnote Cont. From Previous Page)

[8] Verizon relies on the third of three waiver provisions in the PAP. The other two are not apposite here.

[9] Webster's New Collegiate Dictionary defines "clear" as, *inter alia*, "free from obscurity or ambiguity," and "free from doubt." It defines "convincing" as, *inter alia,* "having power to convince of the truth, rightness or reality of something." Black's Law Dictionary defines "clear and convincing proof" as "generally … proof beyond a reasonable, *i.e.*, a well-founded doubt." Verizon has not met its burden of persuasion under the PAP here.

appears to have been typical of these companies." (Petition at 11). First, there are many other companies that **did not** experience systems failures because of the Slammer Worm. Second, Verizon owes a higher standard of care than most ordinary corporations, because of the criticality of its wholesale services to allow CLECs to compete for local exchange customers in Virginia, and because the PAP is a vital component of the market structure created by the Act that has allowed Verizon to enter the interexchange market in Virginia.

For its part, AT&T can say that it did not experience problems of the kind that Verizon experienced. Services to AT&T's wholesale customers such as ATM, Frame Relay, hosting, and wholesale voice were not materially impacted. Nor were there any material impacts to AT&T's command and control systems or customer care services. Verizon seems quite alone in its claims concerning the Slammer Worm.

More fundamentally, of all the companies cited in its waiver request, Verizon is the only one that is a monopoly provider of wholesale services to potential local exchange competitors that is seeking relief from otherwise applicable regulatory penalties for failing to meet its service obligations.[10] It equally bears noting that while Verizon points to a number of other large companies that allegedly had problems, Verizon does not assert that any these firms were relieved of any contractual or regulatory service obligations to customers because of the Slammer Worm, which is the relief it seeks here.

---

[10] While Verizon does mention BellSouth, AT&T is not aware that BellSouth has sought relief from applicable performance assurance measures as a result of the Slammer Worm; nor, to AT&T's knowledge, has SBC or Qwest.

The Commission should also reject the suggestion that it is "highly irregular" that someone might disseminate a computer virus via the Internet. (Petition at 4). The release of such viruses is an unfortunate, but commonplace reality of the Internet. The occasional release of such viruses is no more extraordinary than the possibility that a thief in a parking lot might be tempted to take from an unlocked car an item left in plain view. It is a known risk, and there were known means of effectively eliminating the risk.

The PAP, of course, contemplates waivers for events whose risk cannot be effectively addressed through reasonable precautions, such as **"**catastrophes, natural disasters, [and] severe storms."[11] The waiver process is wholly inappropriate in situations in which Verizon's lack of care results in a substantial deterioration of the service it provides to its competitors.

Given the importance of the PAP's self-executing standards, precedents that have the effect of vitiating their force should be avoided except upon clear and convincing proof of an event for which no amount of reasonable preparation could have mitigated the performance failure. In this case, Verizon merely asserts that the event was not foreseeable. However, the facts are actually otherwise.

Moreover, even when one looks closely at what Verizon does attempt to show, Verizon's claims and proof only cast further doubt on Verizon's actions and arguments. Verizon's basic defense of its actions is that it was reasonable for Verizon to do nothing in advance to address its known software vulnerability, because it would have been challenging to acquire, install, test, and deploy a preventative software patch that Verizon admits was generally available long

---

[11] PAP at 23.

before the Slammer Worm attacked. This purported justification fails to show that Verizon exercised "reasonable, prudent judgment, in operating and protecting its cyber facilities." (Petition at 11). Verizon, by its own admission, made no effort to actually acquire, install, and test the software patch prior to January 25, 2003, even though several iterations of patches were available, the first as early as July, 2002. Verizon has not shown by any standard of proof – let alone clear and convincing proof – how challenging it would have been for Verizon to test and deploy the patch prior to that date.

The fact that Verizon was able to test and deploy the patch in less than two days *after* the incident strongly suggests that Verizon could have deployed and tested the software patch in the same two-day interval during the months that preceded the incident – if Verizon had chosen to do so.[12] Verizon's boasts about the speed with which it delivered its pound of cure also show how painless the ounce of prevention likely would have been.

Demonstrating just how unreasonable Verizon's delay was from an IT perspective is Microsoft's warning system. The Microsoft security bulletins rated the risk "critical" and specifically warned -- as if speaking directly to Verizon about this incident – that

> [i]n industry experience attacks that impact customers' systems rarely result from attackers' exploitation of previously unknown

---

[12] In fact, Verizon did much more than simply test and deploy the software patch where necessary in the 40-hour period beginning at l:00 a.m. EST on January 25, 2003. Verizon also detected network flooding, identified the sources of traffic generation, isolated and quarantined its internal data networks, quarantined external networks, brought down four separate wholesale interfaces, notified CLECs by e-mail and by phone, and identified and removed infected devices, in addition to incrementally deploying the patch. Petition, at 4-5. Merely testing and deploying the patch would have taken Verizon considerably less than two days.

> vulnerabilities. Rather . . . attacks typically exploit vulnerabilities for which patches have long been available, but not applied.[13]

Far from being adrift in a sea of uncertainty about the priority that should be given to applying the patch that would have prevented the incident, Verizon completely ignored urgent, specific, and repeated warnings about the vulnerability of the software systems Verizon uses. These warnings identified the specific consequences that resulted here and came from a highly reliable source -- the purveyor of the software.[14]

Given the vital public interest in the PAP's performance requirements being *effectively* "self-executing," the Commission must reject attempts by Verizon to undermine the forcefulness of those requirements through contrived "extraordinary" events. The Commission must not only reject Verizon's instant effort to side-step the financial consequences of those requirements but should also state with unmistakable clarity that it will not entertain similar frivolous attempts to defeat the PAP's key tools for promoting local competition.

---

[13] See: http://www.microsoft.com/technet/security/policy/rating.asp.

[14] To put Verizon's delay in further perspective, the Commission need only consider Verizon's regular schedule for systems updates. Every Sunday, PAP measures for interface availability are suspended, affording Verizon the opportunity to make modifications and upgrades to its OSS systems without PAP consequences. Between October 2, 2002 and January 25, 2003, Verizon had 17 opportunities to test and deploy the patch issued with Security Bulletin MS02-056 on a Sunday, without PAP consequences. Between October 16, 2002 and January 25, 2003, Verizon had 15 opportunities to test and deploy the patch issued with Security Billeting MS02-061 on a Sunday, without PAP consequences. Thus, Verizon wasted literally half a month of Sundays while not testing and deploying the patches.

Conclusion

For the reasons stated herein, the Commission should reject Verizon's Petition.

AT&T COMMUNICATIONS OF
VIRGINIA, LLC

By: _____
Mark A. Keffer
Ivars V. Mellups

Its Attorneys
3033 Chain Bridge Road, 3D
Oakton, Virginia 22185-0001
703-277-7343

Dated: April 9, 2003

Attachments

April 9, 2003

Joel H. Peck, Clerk
Document Control Center
State Corporation Commission
1300 East Main Street
Richmond, VA 23219

Ex Parte: Establishment of a Performance Assurance Plan for
Verizon Virginia Inc.

Case No. PUC-2001-00226

Dear Mr. Peck,

Enclosed for filing with the Commission are an original and fifteen copies of the Comments of AT&T Communications of Virginia, LLC to the Petition of Verizon Virginia Inc. for a Waiver of Certain Service Quality Results Measured Under the Performance Assurance Plan for January 2003.

Thank you for your attention to this matter.

Sincerely,

Mark A. Keffer

CC: Service List

CERTIFICATE OF SERVICE

Virginia Case No. PUC-2001-00226

I hereby certify that a copy of the Comments of AT&T Communications of Virginia, LLC was sent via U.S. mail, postage prepaid, this 9th day of April, 2003 to the following:

David A. Fitts
Choice One Communications
100 Chestnut Street
Suite 800
Rochester, NY 14604

Thomas Sokol
Sprint Communications
1108 East Main Street
Suite 1200
Richmond, VA 23219

Todd Murphy
US LEC
6801 Morrison Blvd.
4th Floor
Charlotte, NC 28226

Kimberly Wild, Esq.
WorldCom, Inc.
1133 19th Street, NW
Washington, DC 20036

John Spilman
Broadslate Networks, Inc.
675 Peter Jefferson Parkway
Suite 310
Charlottesville, VA 22911

John Knapp
Verizon Virginia
600 East Main Street
11th Floor
Richmond, VA 23219

Stephen C. Spencer
Director – Regulatory & Govt. Affairs
Verizon South, Inc.
600 East Main Street
11th Floor
Richmond, VA 23219

Raymond L. Doggett, Jr.
Assistant Attorney General
Insurance & Utilities Regulatory Sec.
Office of the Attorney General
900 East Main Street
Richmond, VA 23219

Valerie Evans
Covad Communications
600 14th Street, NW
Suite 750
Washington, DC 20005

Robin Cohn
Focal Communications Corp. of
Virginia and Starpower
Swidler Berlin Shereff Friedman LLP
3000 K Street, NW
Suite 300
Washington, DC 20007-5116

Peggy Rubino
Z-Tel Communications
601 South Harbour Island Blvd.
Suite 220
Tampa, FL 33602

Darrell Mennenga
ALLTEL Communications, Inc.,
Virginia Cable
One Allied Drive
Little Rock, AR 72202

Richard A. Schollmann
Virginia Cable Telecommunications
1001 East Broad Street
Richmond, VA 23219

Debbie Jaggard
Cox Virginia Telecom
4585 Village Avenue
Norfolk, VA 23502

Jennifer Anderson
Adelphia Business
121 Champion Way
Cannonsburg, PA 15317

Donald Sussman
Vice President Regulatory Affairs/
Vendor Relations
Network Access Solutions
13650 Dulles Technology Drive
Herndon, VA 20171

Chana S. Wilkerson
Advanced Technology Group, Inc.
of Virginia
901 Dulaney Valley Road
Dulaney Center II
Towson, MD 21204

Scott Golden
Cavalier Telephone
2134 West Laburnum Avenue
Richmond, VA 23227

Steve Goodman
NTELOS
401 Spring Lane
Suite 300
Waynesboro, VA 22980

John McLaughlin, Jr.
KMC Telecom, Inc.
1755 North Brown Road
Lawrenceville, GA 30043

Michael Clancy
Covad Communications
625 Locust Street
Suite 1
Garden City, NY 11530

Kathleen Cummings
Deputy Director
Division of Communications
VA State Corporation Commission
1300 East Main Street, 9th Floor
Richmond, VA 23219

William Irby
Director
Division of Communications
VA State Corporation Commission
1300 East Main Street
Richmond, VA 23219

Steven C. Bradley
Deputy Director
VA State Corporation Commission
1300 East Main Street
Richmond, VA 23219

_____
Danny W. Long