April 18, 2003

Mr. Joel H. Peck, Clerk
State Corporation Commission
Document Control Center
Post Office Box 2118
Richmond, Virginia 23216

Dear Mr. Peck:

Re: Case No. PUC-2001-00226

Enclosed for filing is the original and fifteen (15) copies of Verizon Virginia Inc.'s Reply Comments in the above-referenced case.

I have e-mailed, mailed or hand-delivered copies to the parties shown below. Thank you for bringing this matter to the attention of the Commission.

Very truly yours,

Enclosure

Copy to:
William Irby (letter only)
Kathleen A. Cummings
Service List

BEFORE THE
STATE CORPORATION COMMISSION
OF THE COMMONWEALTH OF VIRGINIA

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.	**:**	

REPLY COMMENTS OF VERIZON VIRGINIA INC.
ON ITS PETITON FOR A WAIVER OF CERTAIN SERVICE QUALITY RESULTS
MEASURED UNDER THE PERFORMANCE ASSURANCE PLAN FOR JANUARY 2003

Verizon Virginia Inc. ("Verizon") provides the following reply to comments made by two CLECs – AT&T and Worldcom – on Verizon's request under the "Performance Assurance Plan Verizon Virginia Inc." ("PAP") for a waiver of certain service quality performance results caused by the Slammer Worm attack. The arguments raised by the CLECs in opposition to Verizon's waiver request are without merit. The Commission should grant Verizon's requested waiver. Verizon further asks that the Commission enter a stay of Verizon's obligation to issue January 2003 PAP credits resulting from the Slammer Worm attack until the Commission has ruled on Verizon's waiver request.

First, the CLECs claim that the Slammer Worm attack was not an "extraordinary" event beyond Verizon's control. Rather, they claim that the attack was a foreseeable event, which should not fall under the PAP's waiver provision. The CLECs are wrong. While it is true that viruses and worm attacks occur frequently, the ferocity of this attack was extraordinary. The Slammer Worm's spread was extremely rapid and affected many large businesses. *See* Verizon Petition at 6 ("the Slammer Worm open[ed] *a new era* of fast-spreading viruses on the Internet . . .") (citation and quotations

omitted); *see also* CNN.com./Technology "Looking into the mind of a virus writer," March 19, 2003 ("the malicious Slammer worm spread across the globe in 10 minutes . . ."). The essential point glossed over by the CLECs is that while viruses and worm attacks may occur continuously, s*ee id*. ("[a]bout 1,000 viruses are created every month by virus writers. . . ."), the Slammer Worm represented a new, much more dangerous breed.

Despite the continuous onslaught of viruses and worm attacks, this is the first time since the PAP was instituted in New York in January of 2000 that a virus or worm has had any impact on Verizon's ability to provide services to CLECs. Moreover, the mere fact that viruses and worm attacks are foreseeable is not a rational basis that would support denial of the Waiver Petition as these CLECs claim. In fact, as Verizon pointed out in its Petition, the New York Public Service Commission ("NY PSC") granted a PAP waiver for a Work Stoppage in August 2000, though work stoppages are foreseeable. *See* Verizon Petition at 9 and note 7. In essence, the CLECs argue that Verizon should be held strictly liable when it has not been able to satisfy a PAP standard due to outside circumstances. The NY PSC rejected similar arguments when it approved the 2000 Work Stoppage Waiver.[1] This Commission should reach the same result here.

Second, AT&T and Worldcom claim that Verizon is not entitled to a waiver because the Slammer Worm attacked a known vulnerability in Microsoft's SQL Server 2000, and that Microsoft had developed a patch for this problem months ago, which Microsoft had designated as a "critical"

[1] Case 99-C-0949, *et al., Petition of Bell Atlantic - New York for Approval of a Performance Assurance Plan and Change Control Assurance Plan, filed in C 97-C-0271*, "Order Granting in Part and Denying in Part Requests for Waivers of Service Quality Targets" (issued June 7, 2001), at 4-5.

patch. Worldcom at 3-4; AT&T at 4-7. AT&T goes to great length to quote from various Microsoft bulletins regarding the application of security patches and states that the Commission need only consider the practices of Microsoft in evaluating whether Verizon acted in a prudent manner. AT&T at 13-14. Verizon agrees that Microsoft's experience is instructive. But it is Microsoft's actions, not its words, that are most informative – particularly Microsoft's inability to protect its own systems and networks from the Slammer Worm despite the availability of patches that Microsoft deemed to be critical. Despite AT&T's contentions that patch management is a snap and that Verizon could have easily installed the necessary patch, industry observers have made it clear that "Microsoft's own actions show that you can't reasonably expect people to be able to keep up with patches." Verizon Petition at 12 (quotations and citations omitted). Penalizing Verizon for failing to fully install a particular patch – even a so-called "critical" one – that was not even fully installed by its maker would be patently unreasonable.[2] Indeed, in the aftermath of the Slammer worm, security experts suggested that such attacks are "inevitable" and that companies should "focus on limiting their damage, rather than expending every effort trying to create an ironclad perimeter."[3] Verizon Petition at 13.

The CLECs' arguments are a classic application of 20/20 hindsight. The issue is not whether Verizon *could have* installed the patch but whether it reasonably could have known that it *should* install

[2] Moreover, the "critical" designation is hardly the red alert that the CLECs make it out to be. The CLECs fail to mention that Microsoft designated as "critical" fully 35 of the 72 security patches it issued in 2002 and five of the nine security patches it has issued thus far in 2003.

[3] Verizon does not claim that the mere dissemination of computer viruses over the Internet is an "extraordinary" event. But Verizon cannot possibly be expected to know in advance – always and without fail – which of those multitudes of viruses are about to attack and should be given the highest priority.

that particular patch, and that it should do so before installing other "critical" patches. The answer to that question is clearly "no." If Verizon had had a crystal ball, and knew that the Slammer Worm was going to attack that specific vulnerability in Microsoft's SQL 2000 Servers slightly after midnight on January 25, 2003, it could have rearranged its IT operations and patch management to test and apply that specific patch to the vulnerable servers in advance of the attack. But Verizon did not have a crystal ball, and could not have known that a worm exploiting that particular defect in MS SQL Server 2000 would be unleashed and therefore that this particular patch should have been given such a super-priority. Thus, the only question is whether Verizon acted prudently before and after the attack. CLEC commenters trivialize and severely underestimate the time and effort required to test and apply the myriad of patches released by software vendors in addition to other systems maintenance activities. Verizon's software vendors announce thousands of patches annually. And, in 2002, Verizon applied over 27,000 software patches to Microsoft servers alone. The internal computing network operated by Verizon and its affiliated companies contains over 233,000 addressable devices. As Microsoft acknowledged, the Slammer Worm required only ***one*** device without the appropriate patch to create the flood of network traffic across the internal computing network. Verizon Petition at 4 (citation and quotation omitted). Contrary to CLEC claims, Verizon has demonstrated that it acted prudently, s*ee id*. at 4-8, and the Commission should not apply 20/20 hindsight to find otherwise.[4]

[4] The only regulatory commission that has yet ruled on Verizon's request for a waiver due to the effect of the Slammer Worm – the Connecticut Department of Public Utility Control – granted that request on March 28, 2003. *See* letter to William D. Smith dated March 28, 2003, in Docket No. 97-01-23. In Maryland, the Staff of the Public Service Commission recently recommended that the PSC grant Verizon's waiver request, on the condition that any future request for a waiver must be based on evidence that Verizon has taken "appropriate steps to inoculate its information systems from viruses . . . ." *See* letter to Felecia L. Greer dated April 4, 2003, in Case No. 8916.

(continued . . .)

Moreover, the interfaces that Verizon specifically developed for the CLECs, in fact, ***were not infected.*** However, at the time of the event, it was apparent that the Slammer Worm was attacking the Verizon internal computing network from outside, and Verizon therefore shut down connectivity paths to external entities, including, but not limited to, the wholesale interfaces.

AT&T's argument that its ATM, frame relay, hosting and voice services to its wholesale customers were not affected is irrelevant. This was also true for Verizon. As Verizon stated, it was Verizon's internal computing network that was affected, not its commercial networks. *Id*. at 6. What AT&T conveniently fails to mention is that AT&T's *internal systems* were indeed infected by the worm, based on AT&T's responses to a post-attack inquiry by Verizon. Also, AT&T implies that Verizon's retail operations were not impacted. This is not true. Since the Slammer Worm impacted Verizon's internal computing network, it impacted both the wholesale and retail systems that use that computing network.[5]

AT&T's statements that "Verizon simply chose not to familiarize itself with Microsoft's warnings or, if it did, simply chose not to take the warnings seriously," and that "Verizon . . . made no effort to actually acquire, install, and test the software patch prior to January 25, 2003," AT&T at 6 and 13, are

---

(. . . continued)

[5] For example, both Wholesale and Retail use that network to access the same back-end systems for ordering. *See* Carrier-to-Carrier Guidelines, Metric PO-2 "OSS Interface Availability" ("Verizon Service Representatives and CLEC Service Representatives obtain Pre-Ordering information from the same underlying OSS"). If anything, this incident highlights the better-than-parity service Verizon is required to provide to CLECs. The attack occurred on a Saturday, which is not considered "prime time" for Verizon's retail operations, but is considered as "prime time" for the purposes of calculating Metric PO-2, even though experience clearly shows that Saturdays are not in fact high-use days by CLECs.

likewise untrue. Verizon, Microsoft, CERT and other industry members were aware of several security vulnerabilities in MS SQL Server 2000. In this particular part of Microsoft's code, there were three known buffer overflow vulnerabilities and one weak permissions vulnerability about which Verizon and others were aware. In July 2002, Microsoft released a "stand alone" patch, designated as "critical" that addressed one of the buffer overflow vulnerabilities. That patch, however, left the other two buffer overflow vulnerabilities and the permission vulnerability open.[6] Microsoft did not release Service Pack 3 (SP3), which corrected all of these defects (among others) and included the tools typically appropriate for patch installation, until almost six months later on January 17, 2003. Verizon had obtained SP3 and was in the process of evaluation and testing it when the Slammer Worm struck on January 25, 2003. Verizon had installed the patch on some of its devices before January 25, 2003, but as noted above, Microsoft itself admits that "it only took one machine" to let the Slammer Worm in.

When Microsoft gave notice of the vulnerability in its software, Verizon was in the position of a person who learns that at some future date a virus that *may* make him ill *may* come into being, but that there is a treatment available that *may* be effective in preventing the disease. However, the treatment will require substantial time and expense, and may have significant adverse side effects. In such circumstances, the person cannot be faulted for proceeding in a cautious and deliberate fashion by ascertaining whether the treatment is effective and will not have adverse side effects before undergoing the treatment.

[6] Also, AT&T notes in its comments that in some circumstances the patch interfered with SQL server operations. AT&T Comments, at 5. Worldcom suggests that Verizon might also have blocked "UDP port number 1434 at the firewall." Worldcom Comments, at 4. However, this would have removed a communications channel from operation.

Finally, the CLECs' overblown claims that the Slammer Worm had a discriminatory, anticompetitive, or financial impact should be rejected. This Commission and other commissions have made it clear that the metrics in the PAP should be used to determine whether CLECs are receiving adequate service from Verizon. Verizon's performance is not evaluated on an incident basis, as the CLEC comments would imply. Instead, its performance is measured under the various standards and time frames in the PAP. A review of the numerous pre-order, provisioning and maintenance metrics included in the January 2003 PAP monthly report demonstrates that Verizon provided CLECs with exceptional service. In particular, Verizon provided a high quality of service on the PO-1 "Response Time OSS Pre-Ordering Interface" submetrics that are included in the PAP, for both January and February 2003. Indeed, the CLECs opposing Verizon's waiver request have not claimed that they were attempting to access Verizon's pre-order systems on Saturday, January 25, 2003. In fact, only one CLEC (which was neither AT&T nor Worldcom) notified Verizon that it was experiencing difficulty using a Verizon interface as a result of the network flooding caused by the Slammer Worm. Thus, it does not appear that the CLECs opposing Verizon's waiver request were adversely affected by the unavailability of Verizon's interfaces on that Saturday. Moreover, although Verizon's electronic interfaces are available on weekends, ordering and provisioning requests received on Saturdays are treated as having been received on the next business day for the purposes of providing services, which in this case was Monday, January 27, 2003. Further, press reports and Verizon's anecdotal information indicate that to the extent the systems of these CLECs relied on Microsoft's SQL Server 2000 and shared Internet-attached networks, they too were dealing with the fallout of the Slammer Worm on and after January 25, 2003.

* * *

The CLECs have not established a valid basis to deny the request of Verizon for a waiver of the PO-2-02 metric performance results for January 2003 that were adversely impacted by the Slammer Worm attack. Verizon is vigilant in protecting the security of its physical and cyber assets and has repulsed countless attempts to violate that security. Yet despite its best efforts, Verizon was unable due to the Slammer Worm attack to satisfy the service quality standards for the PO-2-02 metrics in the PAP for January 2003. Accordingly, the Commission should grant Verizon's waiver request.

Respectfully submitted,

_____

Jennifer L. McClellan

600 East Main Street, 11th Floor
Richmond, Virginia 23219
Telephone No. 804-772-1547

Attorney for
Verizon Virginia Inc.

Dated: April 18, 2003

CERTIFICATE OF SERVICE

I hereby certify that on this 18th day of April, 2003, a copy of Verizon Virginia Inc.'s Reply Comments in Case No. PUC-2001-00226 was sent as stated below:

Don R. Mueller, Esquire
State Corporation Commission
Office of the General Counsel
Post Office Box 1197
Richmond, Virginia 23218
(Hand-delivered)

C. Meade Browder, Esquire
Office of Attorney General
2nd Floor
900 East Main Street
Richmond, Virginia 23219
(U.S. Mail)

Performance Standards/Remedy Plans Subcommittee of the Collaborative Committee
(E-Mail)

_____
Jennifer L. McClellan