

April 8, 2003

***Via Overnight Mail***

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

***Re: Case No. 2001-00226***

Dear Mr. Peck:

Enclosed please find an original and fifteen (15) copies of the Comments of WorldCom, Inc. filed in the above referenced proceeding. Please do not hesitate to contact me if you have any questions regarding this filing. Thank you for your attention to this matter.

Sincerely,

Kimberly A. Wild

Cc: Kathleen Cummings  
Don Mueller  
Service list (via email)

**BEFORE THE  
STATE CORPORATION COMMISSION  
COMMONWEALTH OF VIRGINIA**

<b>Commonwealth of Virginia, ex rel.</b>	)	
	)	
<b>State Corporation Commission</b>	)	<b>Case No. 2001-00226</b>
	)	
<b><u>Ex Parte: Establishment of a Performance</u></b>	)	
<b>Assurance Plan for Verizon Virginia, Inc.</b>	)	

**COMMENTS OF WORLDCOM, INC.**

**INTRODUCTION**

On March 17, 2003, Verizon Virginia, Inc. ("VZ-VA") filed with the State Corporation Commission ("Commission") a Petition for Waiver of Certain Service Quality Results Measured Under the Performance Assurance Plan for January 2003 ("Petition"). Pursuant to the Commission's March 24, 2003 Order in response to the Petition, parties were directed to file comments on VZ-VA's request by April 9, 2003 and VZ-VA was given the opportunity to file reply comments by April 18, 2003. In accordance with the Commission's Order, WorldCom, Inc. ("WorldCom") hereby submits these comments in opposition to VZ-VA's request for a waiver and urges the Commission to deny the Petition for the reasons discussed below.

**DISCUSSION**

The Performance Assurance Plan ("PAP"), which became effective prior to VZ-VA's entry into the long distance market in the Commonwealth of Virginia, is comprised of performance measures and remedies designed to assure the company's quality provision of wholesale service to its competitors on a just and reasonable basis. With

VZ-VA's entry into the long distance market, the PAP plays a critical role in providing VZ-VA with incentives to meet and sustain certain performance standards that are essential to the development and availability of meaningful local competition in Virginia. VZ-VA's failure to meet any or all of the PAP's performance measures not only impedes the ability of competitors to provide service to their customers, but also threatens the very ability of competitors to continue doing business in Virginia. It is with these important considerations in mind that VZ-VA's request to waive certain service quality results should be evaluated.

Specifically at issue here is VZ-VA's request that its performance results in January 2003 be waived for three PAP pre-order measures with absolute standards (the "Pre-Order Measures").<sup>1</sup> In support of its request, VZ-VA claims that an extraordinary event beyond its control prevented it from satisfying these measures. Specifically, VZ-VA contends that: (1) during the weekend of January 25, 2003, certain systems it uses were subject to an internet computer attack by the Slammer Worm, a "self-propagating malicious code that exploits vulnerabilities in Microsoft SQL Server 2000, and certain other Microsoft products[;]"<sup>2</sup> (2) this event hit the network quickly, was beyond its control and occurred without warning; (3) the Slammer Worm attack negatively affected its ability to satisfy the three Pre-Order Measures; and (4) it acted reasonably and prudently under the circumstances, consistent with industry practices in operating and protecting its cyber facilities, adding that patch management to prevent worms from

---

<sup>1</sup> VZ-VA requests waiver of the results for: (1) PO-2-02-6020 "OSS Interface Availability -Prime -EDI;" (2) PO-2-02-6030 "OSS Interface Availability - Prime - Corba"; and (3) PO-2-02-6080 "OSS Interface Availability - Prime - Web GUI."

<sup>2</sup> Petition at 3.

infecting systems is an “extremely complex task.”<sup>3</sup> Because of the impact the Slammer Worm had on its systems, VZ-VA proposes that the affected day - January 25th - be excluded from the calculation of the three Pre-Order Measures for the January 2003 performance month. If granted, the requested waiver would substantially reduce the credits due to CLECs in Virginia from approximately \$1,011,418.00 to \$124,599.00.<sup>4</sup>

Given the critical nature of the PAP to market competitors and end users alike, as well as the potential substantial reduction in credits owed to CLECs for the month of January 2003, VZ-VA’s waiver request warrants thorough scrutiny. However, when subjected to that scrutiny, it becomes clear that VZ-VA’s waiver request should be denied. As specified in the PAP, VZ-VA may file a petition for waiver to have its service quality results modified due to situations *beyond its control* that negatively affect its ability to satisfy only those measures with absolute standards. Among other things, that petition “must demonstrate clearly and convincingly the *extraordinary nature* of the circumstances involved.”<sup>5</sup> VZ-VA has simply failed to make the requisite showing in its Petition.

The Slammer Worm attack at issue here was a foreseeable and preventable event and not an extraordinary event beyond VZ-VA’s control. In fact, Microsoft informed its customers of the vulnerabilities on July 24, 2002. On this date, Microsoft issued a security bulletin (Bulletin MS02-039) to its customers notifying them of vulnerabilities in its Microsoft SQL Server 2000 and Microsoft Desktop Engine (MSDE) 2000 products that, if exploited, could impact customers’ systems. That Bulletin was also widely

---

<sup>3</sup> *Id.* at 11.

<sup>4</sup> *Id.* at 2.

<sup>5</sup> VZ-VA PAP at 23.

distributed by other security alerting services that proactively notify their clients of network/systems vulnerabilities and impending cyber attacks.

Equally as important, Bulletin MS02-039 not only explained the vulnerabilities in its Microsoft SQL Server 2000 and Microsoft Desktop Engine (MSDE) 2000 products but it also explained how to prevent them from being exploited, recommending the use of Patch 056 or the blocking of UDP port number 1434 at the firewall. The Bulletin also rated the severity of the vulnerabilities as “critical.” Microsoft’s “critical” rating of the vulnerabilities ultimately exploited by the Slammer Worm is significant. Microsoft employs a security bulletin severity rating system to help customers decide which patches/fixes they should apply to avoid impact under their particular circumstances and how rapidly they need to take action. Since the severity rating system rates vulnerabilities as “low,” “moderate,” “important” and “critical,” clearly the vulnerabilities rated “critical” are of the utmost concern and require the most immediate attention, *i.e.*, the timely application of patches and fixes. Clearly, the information contained in the Bulletin provided more than adequate notice of the severity of the problem and also provided solutions to block potential attacks.

VZ-VA also attempts to use the speed of the Slammer Worm attack to justify its Petition, claiming that it opened a new era of fast spreading Internet viruses.<sup>6</sup> This is not totally true. Academic researchers had been publishing research on extremely fast virus attacks for at least a year and half before the Slammer Worm struck.<sup>7</sup> The research directly pointed out that since a fast worm can achieve complete spread in well under an hour, and can begin doing damage immediately, human mediated responses offer almost

---

<sup>6</sup> Petition at 6.

no hope of stopping it. Yet, even though warned well in advance by Microsoft and provided with the tools to block the virus, VZ-VA waited until after the Slammer Worm hit and used human-ordered countermeasures to attempt to remedy the problem.

VZ-VA could be - and should be - reasonably expected to keep abreast of critical vulnerabilities and to proactively defend its network and systems against them. While the timing of the Slammer Worm attack itself was beyond VZ-VA's control, proactively protecting its systems was not. To this point, nowhere in its petition does VZ-VA assert that it did not have notice of the vulnerabilities to its systems. VZ-VA should have blocked the specified port or applied the recommended patches that would have prevented the Slammer Worm from infecting its systems. Having failed to do so and thereby protect its systems against a preventable event, VZ-VA cannot be found to have acted in a reasonable and prudent manner. Contrary to VZ-VA's assertions, the Slammer Worm incident was not an extraordinary event that was beyond its control. To find otherwise would inappropriately sanction an extremely liberal definition of "extraordinary" circumstances "beyond VZ-VA's control" on which grounds for a waiver of PAP results may be based. Granting VZ-VA's waiver request would also force CLECs to pay the price for VZ-VA's failure to proactively prevent vulnerabilities to its systems from being exploited by the Slammer Worm. VZ-VA and not CLECs should be held accountable for that failure.

---

<sup>7</sup> Nicholas Weaver, *Warhol Worms: The Potential for Very Fast Internet Plagues* (published August 15, 2001) <<http://www.cs.berkeley.edu/~nweaver/warhol.html>>.

**CONCLUSION**

For the foregoing reasons, WorldCom respectfully requests that the Commission deny VZ-VA's waiver request.

Respectfully submitted,

---

Kimberly A. Wild  
WorldCom, Inc.  
1133 19<sup>th</sup> Street, NW  
Washington, DC 20036  
202-736-6317  
*Attorney for WorldCom, Inc.*

Dated: April 8, 2003