# Exhibit A

**UNITED STATES DISTRICT COURT**
**SOUTHERN DISTRICT OF FLORIDA**
**MIAMI DIVISION**

**CASE NO. 07-22674-CIV-JORDAN**

DELL INC.; AND ALIENWARE CORPORATION,

Plaintiffs,

v.

BELGIUMDOMAINS, LLC, CAPITOLDOMAINS, LLC, DOMAINDOORMAN, LLC, NETRIAN VENTURES, LTD., IHOLDINGS.COM, INC., JUAN PABLO VAZQUEZ a/k/a JP VAZQUEZ, an individual; and DOES 1-10,

Defendants.
_____/

**DECLARATION OF EZEQUIEL GUILLERON IN SUPPORT OF THE REGISTRAR DEFENDANTS' OPPOSITION TO PLAINTIFFS' MOTION FOR SANCTIONS**

I, Ezequiel Guilleron, make the following statements upon my personal knowledge and belief:

1. My name is Ezequiel Guilleron. I am of legal age and sound mind, and competent to make this declaration.

2. I am a telecommunications and information technology technician.

3. I studied computer science at the University of Buenos Aires, Argentina.

4. I am the chief technical officer of Binaria Group, S.A. My responsibilities at Binaria include supervising the development, testing, and implementation of every Binaria Group product.

5. I also provide computer and network security and administrative consulting services to a range of companies including Deloitte & Touche, McKinsey & Company, Telefónica S.A., Teléfonos de México, S.A.B. de C.V., and TIM w.e. New Media Entertainment.

6. I also provide computer security and administrative consulting services to Defendant Netrian Ventures Ltd. ("Netrian").

**Netrian's Routine Security and Privacy Practices**

7. I am responsible for maintaining servers Netrian uses to host the domain name registration services offered by its United States subsidiaries, BelgiumDomains, LLC, CapitolDomains, LLC, and DomainDoorman, LLC (the "Registrars").

8. Netrian's servers are co-located, meaning that they are not located at a physical site owned by Netrian or the Registrars, but rather at facilities provided by Internap Network Services Corporation ("Internap"). The Internap co-location facility Netrian uses is located at 50 NE 9th Street in Miami, Florida.

9. The Registrars' domain-owning registrant customers demand high levels of privacy and security.

10. One of the ways in which the Registrars provide such heightened security and privacy is by deactivating local electronic logging of system activity. This prevents the logging data from being exposed if the Internap servers were to be compromised. It also saves disk space on the Registrars' servers. This is a common security practice among companies of all sizes.

11. Each day Netrian's servers process millions of domain registrations and deletions. Large amounts of temporary disk space are required to store records of those transactions.

12. As temporary data becomes outdated and then deleted, Netrian routinely runs a secure data cleanup program that constantly wipes all disk space, including space from which files have already been deleted (free space).

13. These procedures help to ensure that confidential customer information, such as logins, passwords, and financial information, has been destroyed.

14. However, the combined effect of the Registrars' need for large amounts of available free disk space and commitment to reliability requires that each server have enough space to host temporary data and run applications currently running on other machines. This

permits enough redundancy that any one server's entire load and storage needs can be reallocated to another machine as smoothly as possible in case of failure.

**The NORCO Array**

15. On or about May 28, 2007, Netrian purchased a NORCO-brand RAID storage array. The NORCO array does not itself provide any storage. The NORCO supports up to twelve (12) hard drives. On the same day, Netrian purchased six (6) 750 GB hard drives for use in the NORCO.

16. Then, on or about November 5, 2007, Netrian ordered an additional three (3) 750 GB hard drives for use with the NORCO.

17. As of November 15, the NORCO unit had never been used in a production environment, meaning it had not yet been used to host the Registrar's registration services. The purpose of purchasing the NORCO was to alleviate the storage and redundancy issues identified in paragraphs 11-14, *supra*.

18. Before adding the NORCO array to the online hardware configuration and relying on it on a day-to-day basis, we ran a series of lab tests intended to test its performance. Those tests included the use of several software tools that exercised the array in several tests involving writing zeros, random data, or custom data across all of the disks in the array.

19. These tests measured specific performance metrics including read speed, write speed, cached reads, buffered disk reads, random reads, and random writes. I personally ran all of the tests and concluded with a test that wrote random data across all of the disks in the NORCO array. Accordingly, a surface scan of the disks in the NORCO array following my testing would likely result in totally random data.

20. The intent was to use the NORCO array as the primary shared storage for all twenty two servers. However, until November 6, Netrian encountered technical issues critical to performance that would have affected the quality of service for registrants. Specifically, significant—and unacceptable—latency in writing to disks using NFS protocol was experienced.

21. Therefore, before November 6, 2007, the NORCO array was never attached to a production environment and had never been used in connection with actual services provided by any of the Registrars.

22. That is why, on November 15, 2007, the day of the investigation, the NORCO array was still in the same hardware rack as several other brand-new servers which also had never been used in production environments but on which we had also been running performance tests.

**The Forensic Investigation**

23. When Netrian learned of the pending investigation at the Internap site, it was concerned with minimizing service interruptions to the Registrars' customers during the investigation.

24. The Registrars' customers demand and expect 24/7 service, and even a short outage can cause them, and therefore Netrian, significant problems.

25. In anticipation of the investigation, while careful to not affect any data, I rebooted each server, as I expected the forensic investigators would need to do, to verify whether the servers, once rebooted, could quickly return to service. This was especially concerning as some of the servers had not been rebooted for more than 100 days and I was uncertain as to how a reboot would affect them.

26. At the time of the forensic investigation all Registrar services were fully functional. However, during the investigation Netrian received complaints of service outages from registrants as a result of the actions taken by the investigators.

27. The forensic investigators had full access to all information stored on the servers.

28. None of the data stored on Netrian's servers at the Internap facilities was deleted in advance of the investigation.

29. All infrastructure information was available to the investigators, including the domain name server zone file and all corresponding Internet protocol addresses, all domains used internally, all public domains, and all internal host names (*e.g.*, db, www).

30. None of that information or data was hidden or deleted and is all still intact.

31. All of the Registrars' customer's records were copied and were and still are intact.

32. All of the Registrars' customer's login and password settings were copied and were and still are intact.

33. All of the Registrars' customer's domain name portfolios were copied and was, and still is, intact.

34. All of the programs, databases, scripts, and registry access tools necessary for the Registrars' normal operation were located and copied intact.

35. The full list of currently active and recently registered or deleted domains (which can also be independently verified domain-by-domain by comparing our database and Verisign, Inc.'s) was successfully copied.

36. I am not aware of any particular electronic file, or category of file, which would have been present on the servers during the normal course of business which was not both present at the time of the investigation and available for the investigators to copy.

37. In the days before the investigation, I am aware of no atypical behavior by anyone apart from the rebooting which was performed to minimize customer inconvenience during the investigation.

I declare under penalty of perjury that the foregoing is true and correct.

Signed on this 22nd day of January, 2008.

Ezequiel Guilleron