netVigilance, Inc. | 14525 SW Millikan Way #34423 | Beaverton, OR 97005 | 503.524.5758

***** For Immediate Release *****

New PCI Compliance Rules To Impose Significant Burdens on Merchants

netVigilance Issues Urgent Bulletin:
Ten Actions Merchants Must Immediately Take To Avoid PCI Failure

Beaverton, Oregon – March 17, 2010 – netVigilance, the only vulnerability assessment and PCI Approved Scanning Vendor (ASV) vendor that goes Beyond Compliance to detect up to 97% of all common vulnerabilities, today issued an urgent bulletin warning all merchants and retailers subject to PCI-DSS Compliance that new PCI regulations significantly increase their chances of PCI failure during mandatory quarterly external vulnerability scans, unless the merchants take corrective actions. netVigilance CTO Jesper Jurcenoks noted, "While these new regulations officially go into effect on September 1, 2010, preparing for them can take months. The time to start is now, because merchants who wait will be at a high risk of failing and being unable to quickly remediate."

The need for this bulletin arose because on March 15, 2010, the PCI Security Standards Council's (PSI SSC) released "ASV Program Guide v1.0," which tightens and changes existing rules governing both customers requiring PCI scans and the Approved Scanning Vendors (ASVs) who perform those scans. netVigilance also calls attention to the fact that, despite being numbered as v1.0, the new ASV Program Guide governs PCI v1.2 and enhances, improves and supersedes the Technical and Operation Requirements for ASVs v1.1 and Security Scanning Procedures v1.1.

Ten Actions Merchants Must Immediately Take To Avoid PCI Failure

1. **Ensure and verify previously out-of-scope components will pass PCI before your next quarterly scan**. New discovery procedures compel merchants to include components previously not in scope–components such as spam filters, mail servers, and non-credit card processing web servers.

2. **Ensure that your hosted environment obtained a "pass" on its ASV scan or get written permission enabling you to scan them. If your ISP will not grant permission or cannot pass, you must change to one who will.** It is now the merchant's responsibility either to obtain proof from each of their hosting and services providers that the entire infrastructure has passed PCI, or to obtain written permission to scan them. Web hosting, mail hosting, spam filtering, etc. are all included.

3. **Remove otherwise secure database servers directly on the Internet by placing them behind firewalls.** Having such servers publicly available is now automatically deemed a PCI failure.

4. **Scan your website specifically for HTTP Response splitting/header injection.** Use a qualified vulnerability assessment company such as netVigilance; if problems are found, they can help you remediate the problem.

5. **Verify that the DNS server holding your domains does not allow DNS Zone Transfers**. (A DNS Zone Transfer allows a third party to obtain lists of all the servers that comprise your domain, even the servers you have not told anybody about.) Regardless of whether someone else hosts your domain, this is still a new automatic PCI failure. Use a qualified vulnerability assessment company such as netVigilance; if problems are found, they can help you remediate the problem.

6. **Make sure your ASV does not rely on a fully automated process to keep pricing low, because the new rules mandate that each and every scan be reviewed by a professional Security Engineer qualified by PCI.** Many ASVs keep prices low by relying exclusively on a fully automated process. Under the new rules, this will no longer be permitted. This is a significant change in procedure that will incur a non-trivial cost, because the review cannot be done by cheap labor, but only by a Security Engineer with several years of experience. netVigilance already follows this procedure and will not increase prices. However, merchants currently using low-cost PCI ASVs must expect an increase in price, as well as longer delivery times.

7. **First, turn off SSL v2. Then ensure that servers using TLS v1.0 or newer are not backwards compatible with the weak SSL v2.**, A competent ASV will verify this and help you remediate.

8. **Remove all non-critical uses of all remote access software, such as pcAnywhere, VNC, and RDP (including VPN).** On critical uses, ensure strong authentication.

9. **Move all Point of Sale (POS) systems behind the firewall**. ASVs are now required to pay extra attention to discovered POS systems.

10. **A specific employee must now put his or her name on the line to attest that "proper scoping of the external scan is 'my company's'" responsibility.** Previously, it was possible to avoid having any named individual be responsible for scoping, which led to frequent improper, overly narrow scoping.

About netVigilance

netVigilance is the fastest growing vulnerability detection and assessment company, because it goes Beyond Compliance to identify and detect up to 97% of common network vulnerabilities, far more than any competitor. Among security companies, only netVigilance focuses exclusively on solutions for Network Vulnerability Detection and Assessment, including PCI Compliance. Further, only netVigilance is an active member of both the PCI ASV Task Force and the CVSS SIG under first.org, where it leads industry efforts to improve these key standards. netVigilance's Total Coverage, Total Coverage PCI, Total Vigilance, and Total Vigilance PCI solutions all go Beyond Compliance to provide customers with both the industry's best detection of common network vulnerabilities and the most detailed remediation reports. For more information, visit www.netvigilance.com.

netVigilance Press Contact:
Steven Mason
650-776-7968
steven.mason@netvigilance.com

Please note: Mr. Jurcenoks is available for interviews on this urgent bulletin and on all aspects of PCI-DSS Compliance.

###