Policy Re: Review of Client Security Scans,
and Penetration Test Results

As you may know, we are a certified PCI service level 1 provider (the highest level there is). This allows us to be listed on both the Visa and Mastercard websites (search for "Nexternal"). We spend a lot of money on this certification, which requires us to go through multiple annual security audits. At the end of each year's rigorous testing and audit, we are awarded an *Attestation of Compliance* by our PCI approved security assessor, Security Metrics, which you can access in the Training & Resource Center under "Security".

From time to time clients ask us to review "failed" results of security scans required by customer payment processors, or customer-initiated security scans. Researching each of these fails often takes a good bit of time and resources, which represents additional expense to us, yet they are almost always false positives or the result of misinterpretation.

Therefore, the first thing you should do when presented by fail reports in these circumstances, is to supply your tester with our Attestation of Compliance. This should be enough evidence that we are in full compliance with the PCI rules and regulations. You can download the current Attestation of Compliance from the Training Center in your OMS.

If your testing company is not satisfied with that evidence, and you wish for us to review the issues, you will need to forward the full report provided by your testing company to your account manager, and your account manager will pass it on for review by our security team.

Those security review services will be performed at $150/hr with a 1-hour minimum. If an issue is found to have merit warranting a change to our environment, then the $150/hr rate for the research related to it will be waived. If an issue is a false positive or a misinterpretation, you will be billed on your next invoice for the time our security team spends investigating the issue and providing you with a response that you can pass along to the vendor that initiated your scans.

In the event that you wish to conduct your own penetration testing, please coordinate the dates with your account manager well in advance, and provide your account manager with the IP addresses from which you will be conducting the tests. Questions and comments from your penetration testing vendor will be billed in accordance with the above.