The Franchise Valuations Reporter

404 Park Avenue South, 16th Floor, NY, NY 10016
O: (212) 689.0400 / Bruce@FranchiseValuations.com

Volume 1, Issue 6 – July 2009

Welcome to our newsletter focusing on issues unique to our practice with respect to franchising, dealerships and distributorships: valuation and damages, cyber crime, expert testimony and tax nexus. We hope you find information that warns, informs and benefits you.

Bruce S. Schaeffer, Editor
Bruce@FTRM.biz

Nexus Notes

DANGER! New York Tax Law Change Requiring Information from Franchise Systems

Franchise companies must be aware that somehow – with absolutely no input from the franchise community, as very ably reported by David J. Kaufmann, Esq. in the *New York Law Journal* - the State of New York just recently passed a budget bill amending Section 1136 of the Tax Law to mandate that all franchisors file information returns giving the names and addresses of all their franchisees in the State.

Far more ominously the legislation provides that future forms under the same statute will require information on all payments from the franchisees to the franchisors and records of all sales from the franchisors to their franchisees with the first returns due September 20, 2009 covering the period March 1 to August 31.

Organizations such as the International Franchise Association have shown a somewhat nonchalant response to the new legislation merely advising their constituency to file the requested information without further counseling that they very carefully research their situation first.

The IFA has continued its advocacy for a federal law change requiring "physical presence" (as opposed to "economic nexus") to yield tax liability. But realistically such an initiative has no chance of prevailing. There have been years of nowhere legislative proposals and repeated attempts at getting U.S. Supreme Court review - all have failed. And the IFA has also claimed that the recent NY law change is unconstitutional.

Neither of these positions has any chance of providing timely benefit for the franchise

community - the due date for the returns is less than 70 days away and the chance of winning a constitutional challenge or amending the law in that period of time is spit to none.

So we recommend very strongly that franchise systems make no mistake about this: the information returns which will be provided to NY State will, for all intents and purposes, effectuate a sales tax audit of all the NY franchisees and an income tax (and possibly sales tax) audit of the franchisors.

Thus, we cannot recommend too strongly that franchise systems collect, analyze and most importantly compare the information collected before filing any reports.

And because the sharing of this kind of information could be used to create in-system disputes (e.g. underreporting claims, etc.) we recommend very strongly that franchise systems engage a neutral entity (such as us) to act as intermediary to gather the information from both sides without fear of having it used in an adversarial way. After determining whether and to what extent there is exposure for past tax liabilities, a strategy can be adopted and a palatable and protective settlement can be negotiated with the tax authorities as soon as possible.

We have differed for decades with the IFA's position on the issue of nexus, and feel that such history only makes us more effective because we offer the following:

Knowledge - Nationally recognized authority on income and sales tax nexus; Decades of experience with finance and tax aspects of franchising

Credibility - Published position favoring state's authority to tax; No antagonism with state and local tax authorities

Neutrality - Serve ombudsman role to avoid creating internal disputes; Protecting sensitive internal tax and financial information

Actionable Advice - Reconciling disparities before submitting returns; Strategies to manage nexus exposure and potential tax liability, if any

If we can be of any assistance please don't hesitate to contact us.

CyberCrime

No System is Secure - Insider Hacks Goldman Sachs

Goldman Sachs is known for its enormous profits, its sophisticated and profitable computerized trading programs and as the most information security conscious company in the world. They are rumored to have at least six layers of cyber-security. Yet even they were almost victimized by one of their own employees who stole their trading software. In June, a 39-year-old computer programmer Sergey Aleynikov uploaded a stream of code from his desktop at GS to a Web site based in Germany.

According to a *New York Times* account, Aleynikov "was caught when the bank noticed the surge of data leaving its servers — and despite his prowess as a highly paid programmer, his activities were recorded even though he tried to erase his programming commands because Goldman kept back-up records." If the transfer had not been detected, the secret know-how and proprietary code could have been stolen, causing harm not only to Goldman but disrupting U.S. markets as well, according to the U.S. Attorney.

GS is the gold standard in cyber security. If their intellectual property can be compromised – despite multiple layers of security and intrusion detection systems – just imagine how vulnerable a typical franchise system or law firm is.

http://www.nytimes.com/2009/07/07/business/07goldman.html?scp=1&sq=ex-worker&st=Search

A Free Test of Your Website Security

Did you know that Payment Card Industry Data Security Standards, which applies to any business that swipes any plastic cards with a VISA, MasterCard, Discover or American Express logo as payment, stipulates that a company must take special steps to secure its web applications? In other words, you must safeguard your sensitive financial data or face fines, penalties and possibly - even worse - a yearly mandated government audit at your expense.

PCI DSS also requires that companies install an application layer firewall in front of Web applications, or have all custom application code viewed for vulnerabilities by an organization that specializes in application security, such as our FTRM division. The recent PCI DSS update, 1.2, recommends taking both steps simultaneously.

Henfree and Henry Chan, our network security experts, have been testing an interesting product, dotDefender, from Applicure Technologies. Designed for businesses that accept credit card payments on their websites, dotDefender creates a security layer in front of the application, detecting and protecting against internal and external attacks that could compromise the server, steal credit card and other sensitive data, or hack into internal systems.

Get in touch with us today to arrange to download and install a free test of your system which will include a review of your web traffic logs. The download will take 30 minutes or less to install and the results will be very surprising. Call us at 212.689.0400 or e-mail Henry@FTRM.biz or Henfree@FTRM.biz.

MORE REASONS TO BE FRIGHTENED!

Links to Recent Articles on Cyber-Crime

Laid-Off Associate Joins Computer Hacking Community
http://www.abajournal.com/news/laid_off_associate_joins_computer_hacking_community

Cyberattacks Hit U.S. and South Korean Web Sites

http://www.nytimes.com/2009/07/09/technology/09cyber.html?_r=1&hp