404 Park Avenue South, 16th Floor, NY, NY 10016
O: 212.689.0400 / Bruce@FranchiseValuations.com

The Franchise Valuations Reporter

Volume 2, Issue 2 – Feb 2010

Our areas of expertise in the franchise, distribution and dealership context are:
Finance, accounting and tax;
Damages, valuations and expert testimony; and
Cyber-security and E-discovery of ESI (Electronically Stored Information)
We offer a free initial consultation. If any readers have questions, you are welcome to email or phone us and we will provide our best answer as quickly as possible.

Bruce S. Schaeffer, Editor
Bruce@FTRM.biz

Franchisor Income Tax Nexus and FIN 48 Accounting for Uncertain Tax Positions

The IRS announced on January 26, 2010, (Announcement 2010-9) that it would require companies with assets of at least $10 million that file with the SEC to provide information about questionable tax transactions in a surprise move aimed at questionable or illegal tax shelters.

I.R.S. officials said the proposed rule would cover parent corporations and their subsidiaries and related entities, including those overseas, adding that it could be applied to partnerships and other similar entities as well. The agency plans to ask Congress to approve penalties and sanctions for companies that fail to make the annual disclosures. Although the new I.R.S. rule applies only to federal income tax situations, it piggybacks FIN 48, which addresses "accounting for uncertainty in income taxes" and includes uncertainty about state and local taxes as well.

The Financial Accounting Standards Board (FASB) issued interpretation No. 48 - Accounting for Uncertainty in Income Taxes in June, 2006. FIN48 calls for the recognition and measurement of **all** tax positions taken or expected to be taken by **all** U.S. companies. It is effective for fiscal

years beginning after December 15, 2006 and applies to all entities that prepare GAAP financial statements.

According to the AICPA, "The accounting for all material positions taken (or expected to be taken) on any income tax return is governed by FIN 48. Income tax returns include those that were filed or that should have been filed with **local, state**, federal, and international taxing authorities. FIN 48 specifically applies to positions such as: . . . (3**) the decision not to file a tax return in a particular jurisdiction for which such a return might be required**." (emphasis added)

FIN 48 requires companies to determine whether or not a tax position will be sustained upon examination by the taxing authority. Upon completing this "more likely than not" assessment on each position taken, companies are required to determine the amount of benefit to recognize in the financial statements. Any differences between tax positions taken in a tax return and amounts recognized in the financial statements will result in an increase in liability for income taxes payable (or reduce income tax refunds receivable) and/or reduce the company's deferred tax assets or increase their deferred tax liabilities.

Certain Practitioners and the International Franchise Association have repeatedly taken the position, and continue to maintain the position, that there is a reasonable argument that absent "physical presence" a franchisor does not have income tax nexus with a jurisdiction – that economic nexus is insufficient for income tax liability.

This position has lost in the courts throughout the country, consistently and repeatedly, since the South Carolina Geoffrey case in 1993 – 17 consecutive years of losses and denials of Cert by the US Supreme Court.

FIN 48 applies to any taxpayer's decision not to file a tax return in a particular jurisdiction for which such a return might be required. How can these people continue to assert there's no income tax nexus without "physical presence" and not specifically advise anyone heeding their advice that they must footnote such positions in their financial statements to make them comply with GAAP?

Nexus Notes

"Physical Presence" Not a Requirement for Gross Receipts (Sales) Tax Nexus – Proposed Statutory Presumption in New Mexico

According to CCH, the New Mexico House of Representatives has introduced a so-called "Amazon" bill that would establish a presumption that certain Internet sales of goods and services are subject to the state's gross receipts tax. If enacted, the bill would provide that a person having a business with no physical presence in New Mexico would nonetheless be presumed to be engaging in business in New Mexico and would have nexus with the state if: (i) that person enters into an agreement with a resident of the state under which the resident, for a commission or other consideration, directly or indirectly refers potential customers, whether by link or an Internet Web site or otherwise, to that person; and (ii) the cumulative gross receipts from sales by that person to customers in the state who are referred to that person by all

residents with an agreement are in excess of $10,000 during the preceding 12-month period ending on June 30 of any year. (H.B. 50, as introduced in the New Mexico House of Representatives on January 15, 2010)

"Physical Presence" Not a Requirement for Sales Tax Nexus – Proposed Statutory Presumptions in Virginia, Mississippi, Colorado and Vermont

Also according to CCH, other so-called "Amazon" bills have been introduced in the Virginia, Mississippi, Colorado and Vermont legislatures that would provide that a dealer is presumed for retail sales and use tax purposes to be soliciting or transacting business in the respective states by an independent contractor, agent, or other representative if the dealer enters into an agreement with a state resident under which the resident, for a commission or other consideration, directly or indirectly refers potential customers, whether by a link on an Internet site or otherwise, to the dealer. (S.B. 660, as introduced in the Virginia Senate on January 21, 2010; S.B. 2927, as introduced in Mississippi Senate on January 18, 2010; and H.B. 1193, as introduced in the second regular session by the 67th Colorado General Assembly on January 22, 2010; H.B. 661, as introduced in the Vermont House of Representatives on January 28, 2010). All of the newly proposed statutes are modeled on New York's "Amazon" bill which has so far survived court challenge and appeal.

"Physical Presence" Not a Requirement for Income Tax Nexus

CCH also reported that a nonresident shareholder of an Alabama S corporation was subject to Alabama personal income tax when the S corporation merged with another company and the shareholders elected to treat the transaction as a sale of deemed assets under IRC §338. The imposition of tax on income received by the nonresident shareholder did not violate the Due Process Clause of the U. S. Constitution since the receipt of income generated by the deemed sale of assets constituted sufficient connection with the taxing state of Alabama. Although the nonresident taxpayer argued that the tax lacked substantial nexus in violation of the Commerce Clause of the U. S. Constitution, he cited no legal authority sufficient to justify reversal of the trial court's determination other than a general proposition of law. (*Prince v. State Department of Revenue,* Alabama Court of Civil Appeals, No. 2080634, January 22, 2010)

Cyber Security and E-Discovery of ESI

Flip Sides of the Same Coin - Cyber Protection

Simple, Unsophisticated Theft via USB

Did you know the most common theft method used by disgruntled employees for stealing **Electronically Stored Information (ESI)** is those little USB thumb drives that everyone seems to carry? Intellectual property, proprietary databases, customer lists, confidential operating manuals and secret formulas can all be discreetly copied from any computer that has access to the

corporate network. The stolen files can then be used to start a competing business or even sold to a competitor.

When Departing People Steal Company Data: *The Computer Fraud and Abuse Act*

Disgruntled employees or franchisees, when leaving a franchise company, have been known to wrongfully access the company's server and forward to themselves e-mails and other electronic files (or even entire databases). And some – for spite or to cover their tracks – even delete files from the company's server. This can give rise to a lawsuit under the Computer Fraud and Abuse Act (CFAA) 18 U.S.C. § 1030(g).

When this happens the well-counseled franchisor may seek a preliminary injunction that orders Defendants, under the supervision of counsel: (1) to create exact electronic images of all Electronically Stored Information on computer drives and/or other devices in Defendants' possession, custody, or control on which there exists any email, document or other electronic file that was forwarded or otherwise taken from any of the company's computers or servers and to deliver those images to defense counsel for safekeeping until the company's CFAA claim is resolved; and (2) to identify and produce to the company copies of all the Plaintiff's electronic files in Defendant's possession that concern or relate to any business that defendants did as a franchisee, including all the company's electronic files that concern or refer or relate to any confidential information or customer or client with whom defendants worked as a franchisee or for a franchisee. [The CFAA is violated by anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains. . . information from any protected computer," provided that the conduct involved interstate or foreign communication. 18 U.S.C. § 1030(a)(2)(c)].

In order to obtain a preliminary injunction on a CFAA claim, the Plaintiff must generally show the court with specificity: who accessed the company's email system and how emails were sent, deleted, or stored. The Plaintiff must also show that the information it seeks is not available through an analysis of its own server. And the Plaintiff must overcome the argument that the requested relief is simply unnecessary because Defendants, whether in court proceedings or in arbitration, are obligated to preserve any potential evidence anyhow, including electronically stored files.

To deal with this increasing phenomenon – departing employees or franchisees stealing ESI – a Plaintiff (whether or not they can obtain a preliminary injunction) must engage E-Discovery experts – like the Chan Brothers of Franchise Technology Risk Management – to explain the nuances of ESI to counsel, how it is stored, to what degree it can be recovered or not recovered, how imaging of hard drives and devices should be done to preserve a litigation hold and how such image can then be further copied and annotated to provide a searchable database for discovery and trial.

"Friends" Targeted in Cyber Attack

At the end of January, we issued a CyberCrime Alert related to a Los Angeles law firm that was victimized in a sophisticated cyber attack. They were sent e-mails disguised to appear as if they had been sent by other members of the firm. The messages included attachments laden with Trojans and malware that could have

allowed the hackers access to the firm's confidential files.

Following that, we learned that hackers targeted "Friends" of employees within Google China. Basically, hackers identified key employees with access to proprietary data who were also members of various social networks such as Facebook. But instead of attacking them directly, the hackers targeted their friends on these same social networks.

Once those friends were compromised, their accounts sent instant messages with Trojan and malware links to the original target. This was a well thought out plan where reconnaissance was key – targets were mined for their value and roles at the company. Google's internal alarms went off and they followed data breach policies and procedures in order to contain and ascertain the damage. Does your firm have these types of policies and procedures readily available in case of such a breach?

How to protect yourself: Computer users should always be wary of opening attachments or clicking on links in unsolicited e-mails and instant messages from people they don't know. With this new threat, however, even messages from familiar senders may be suspect. Make sure your antivirus and security software are up to date. Also, a Web Application firewall will help defend against certain types of attacks better than your normal firewall. Use the latest versions of operating systems and application software and be diligent about installing patches. Never give out personal information in e-mail, ever.

For those of you doing business on Facebook and other social networking sites, this is a wake-up call. If you have not implemented cyber security policies and training in your organization, you need to start now. We invite you to contact us to learn more about your risks and how to protect yourself.

To arrange a free test of your system, including a review of your web traffic logs, call us at 212.689.0400 or e-mail: Henry@FTRM.biz or Henfree@FTRM.biz.