The
Franchise Valuations
Reporter

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

Volume 1, Issue 8 – September 2009

Damages, Valuations and Cyber Crime

Welcome to our newsletter focusing on issues unique to our practice that we don't think are addressed anywhere else with respect to franchising: valuation and damages, cyber crime, expert testimony and tax nexus –the issues we know best, that matter to our clients - franchise executives and the consultants, attorneys and other professionals who advise them. We hope you find information that warns, informs and benefits you.

Bruce S. Schaeffer, Editor
Bruce@FTRM.biz

If you do not want to receive this e-mail reporter, you may unsubscribe below.

Nexus Notes

DANGER! California Demanding Withholding on Royalties – It's not Just New York Going After Franchisors

As the International Franchise Association's Troy Flanagan alertly advised members in August, the California Franchise Tax Board has recently been contacting non-resident franchisors. Based on discussions with the FTB and member feedback, the IFA learned that state regulators are taking the view that non-resident franchisors must either register with the Secretary of State or have their California franchisees withhold 7 percent of royalty payments.

The FTB's website says (in pertinent part):

"Withholding on domestic nonresidents with California source income

We administer withholding laws pertaining to domestic nonresident payees when any of the following is true:

- **Payee receives California source income that includes, but is not limited to:**
  - Leases
  - Rents
  - **Royalties**
  - Winnings
  - Payouts

Nonresident payees are subject to withholding on California source income regardless of where they live,

enter into a contract, or receive payment."

We reviewed the CA Regulations cited by the State and think Franchisors could have a big problem. Of all the authorities relied on by CA the most dangerous for the franchise community is §17952, which reads in pertinent part:

> "§ 17952.* Income from Intangible Personal Property.
>
> (a) Income of nonresidents from rentals or royalties for the use of, or for the privilege of using in this State, patents, copyrights, secret processes and formulas, good will, trade-marks, trade brands, franchises, and other like property is taxable, if such intangible property has a business situs in this State within the meaning of (c) below.
>
> c) Intangible personal property has a business situs in this State if it is **employed as capital** in this State or the possession and control of the property has been localized in connection with a business, trade or profession in this State so that its substantial use and value attach to and become an asset of the business, trade or profession in this State." (emphasis added)

If the Intangible Property is considered "employment of capital" it can create a nightmare because then franchisors (1) have to value their intangibles (in-state vs. nation-wide) and (2) it affects both nexus and the franchisor's effective tax rate.

Example: F, a successful franchisor, has gross revenues for the year of $100 million. F derives $30 million of its revenues as royalties from CA. F has deductions of $80 million and, therefore, taxable income equal to $20 million. F has no payroll in CA and, arguably, employs no capital in CA. The allocation percentage in CA is computed by determining:

(1) a payroll percentage (in this instance, 0%);

(2) a capital percentage (in this instance, 0%); and

(3) a revenue percentage (in this instance, 30%)

and then adding the various percentages (with the revenue percentage included twice) and dividing the sum by 4. In this case, 0% + 0% + 30% + 30% = 60%, divided by 4 = 15%. Thus, the CA tax is: Net Income ($20,000,000) × Allocation percentage (15%) × Tax Rate (8.84%) = Tax Due of $265,200. That is an effective tax rate on income of 1.33%.

However, if it were found that the value of F is $500 million and that 70% of such value is represented by its trademark and goodwill (a commonplace value allocation in franchise companies), that F's business in CA by licensing its IP constituted the "employing of capital" as embodied in such trademark and goodwill, and that such capital employed were deemed to be in the same percentage as revenues earned (*i.e.*, 30%), then the tax due would be computed as follows: payroll percentage = 0%; capital percentage = (70% of 30%) 21%; revenue percentage

doubled is 30% × 2 = 60%; therefore, allocation percentage = 81% divided by 4 = 20.25%. Thus, Net Income ($20,000,000) × Allocation Percentage (20.25%) × Tax Rate (8.84%) = Tax Due of $358,020. That is an effective tax rate of 1.79%. Therefore, having the trademark deemed the "employing of capital" in CA, on these facts, increases the franchisor's liability by 35% on no increase in income.

But that is nothing compared to the withholding threat at 7% which would yield a CA tax liability of $2,100,000 ($30,000,000 X .07). That yields an effective rate of 10.5% on income and more than 586% of the dollar cost of the next highest potential liability. Thus, the moral of the story clearly is to register and pay CA corporate taxes as a non-resident or they will kill you more than five times over – at least!

The full text of the relevant CA Regulations is available here -
http://www.franchisevaluations.com/press/CA_Regulations.pdf

CyberCrime

The Red Flags Rule and Data Security

This is Part I of a two part posting addressing the FTC's so-called "Red Flags Rule", which requires certain businesses to implement Identity Theft Prevention Programs. First we will review what the Rule is and how it applies to franchises. In Part II we cover implementation and then turn to the larger issue of information security.

The best way to look at the Red Flags Rule is to consider it as merely one component of a comprehensive data security program. Even businesses considered at low risk for identity theft are well advised to take steps to strengthen their defenses against cyber attacks.

What Is the Red Flags Rule?

The Red Flags Rule is an anti-fraud regulation mandated under the Fair and Accurate Credit Transactions Act of 2003 (sometimes referred to as FACTA or the FACT Act) and developed by the Federal Trade Commission and other regulatory authorities. Red flags are defined as patterns, practices or specific activities that indicate the possible existence of identity theft.

Determining whether or not the Rule applies to a business is a two-step process. The Rule requires that "creditors" with "covered accounts" prepare and implement a written Identity Theft Prevention Program. Franchisors and Franchisees are not specifically targeted under the Rule but they may fall within the definition of "creditors" by virtue of their billing procedures and payment mechanisms when dealing with franchisees or customers. If a franchise company regularly permits deferred payments for goods or services, it is probably a "creditor". However, simply accepting credit cards as a form of payment does not make a business a creditor under the Rule.

The Rule was originally scheduled to take effect November 1, 2008, but the FTC postponed the enforcement date three times due, in part, to a lack of clarity over what constitutes a creditor or a covered account. Organizations representing medical practices, lawyers and accountants appealed to the FTC for exemptions but there has been no decision to exempt these entities to date. Enforcement of the Rule is now scheduled to begin November 1, 2009.

Examples of activities which would cause a franchisor or a franchisee to fall within the FTC definition of creditor include:

- Making loans to, or arranging third party financing for, a prospect, a franchisee, or a customer;
- Billing franchisees or customers for products or services after they have been provided;
- Deferring royalty payments (NB: In these hard times many franchisors are extending such relief);
- Charging interest to franchisees or customers for late payments;
- Using consumer credit reports in evaluating prospects (an almost universal practice by franchisors selling franchises); or
- Collecting or processing credit applications for third party lenders (e.g., as auto dealers or retailers may do).

If the business is considered a "creditor," the next step is to determine if it has any "covered accounts." A covered account is "an account used mostly for personal, family, or household purposes, and that involves multiple payments or transactions… A covered account is also an account for which there is a foreseeable risk of identity theft – for example, small business or sole proprietorship accounts." [FTC Business Alert, June 2008, "New 'Red Flag' Requirements for Financial Institutions and Creditors Will Help Fight Identity Theft."] Since a franchisee may be organized as a small business or sole proprietorship with close ties to the personal identity of the owner, the FTC considers such a franchisee to be a "covered account."

Pursuant to the Rule, franchisors and/or franchisees that are properly characterized as "creditors" with "covered accounts" must develop written Identity Theft Prevention Programs to spot and deal with red flags – warning signs that indicate that an identity thief is trying to use stolen personal information. News accounts are full of incidents where thousands, and indeed millions, of personal identities have been stolen electronically by sophisticated cyber-criminal gangs. However, many identity thefts are remarkably low-tech, perpetrated by old-fashioned pickpockets and purse-snatchers. One notorious incident involving Federal Reserve Board chairman Ben Bernanke featured a combination of low- and high-tech activity by a criminal identity fraud ring. [See, Michael Isikoff, "Ben Bernanke Victimized By Identity Fraud Ring," *Newsweek*, August 25, 2009 http://www.newsweek.com/id/213696.]

Some franchisors and franchisees already have measures in place to prevent hackers from gaining access to their electronically stored consumer information. Having such measures, however, does not mean that the organization is in compliance with the Red Flags Rule. The Rule seeks to reduce the damage crooks can inflict both on victims of identity theft and on businesses left with accounts receivable they'll never be able to collect. The Rule "picks up where data security leaves off," according to Manas Mohapatra, an attorney with the FTC. [Colleen McCarthy, "FTC's Red Flags May Color Some Surprised," BusinessInsurance.com, July 26, 2009.]

The Rule itself only covers preventing *the use of* false identities, but any sensible franchise system must consider preventing identity theft in the first place.

What Organizations Need To Do To Comply

The FTC has estimated that there are about 11 million entities that will qualify as "creditors" and thus will be subject to the Rule and the jurisdiction of the FTC. Of these 11 million, about 1.8 million will have "covered accounts" and thus will have to create a written Program. Of these 1.8 million entities, the FTC estimates 266,000 are subject to a high risk of identity theft.

To simplify the process of designing and implementing a written Identity Theft Prevention Program for the 1.6 million covered businesses considered to be at a low risk of identity theft, the FTC has created a 6-page compliance template. http://www.ftc.gov/bcp/edu/microsites/redflagsrule/RedFlags_forLowRiskBusinesses.pdf]

Whether a company subject to the Rule chooses to use the template or not, creating a Program involves four steps. The company must:

1. **Identify** red flags that are likely to come up in that business;
2. Spell out how employees will **detect** such warning signs;
3. Include procedures to **respond** to and mitigate the harm from identity theft; and
4. Provide for periodic **updates** of the program to account for, among other things, technology changes, new methods of operation by identity thieves, and changes in the way the business operates.

Part II will cover implementation of the Rule as well as the general topic of good data security practices.

FTRM can help with designing your entire Identity Theft Prevention Program. Call us at 212.689.0400 or e-mail Henry@FTRM.biz or Henfree@FTRM.biz.

A Free Test of Your Website Security

As we have previously advised, Payment Card Industry Data Security Standards require 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. The recent PCI DSS update, 1.2, recommends taking both steps simultaneously.

Henfree and Henry Chan, our network security experts, are offering a complimentary testing of your internet facing structure using, 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 a free test of your system which will include a review of your web traffic logs. It will take 30 minutes or less and the results will be very surprising. Call us at 212.689.0400 or Henry@FTRM.biz or Henfree@FTRM.biz.

MORE REASONS TO BE FRIGHTENED!

Links to Recent Articles on Cyber-Crime

U.S. Indicts 3 in Theft of 130 Million Bank Cards [Hannaford, 7-eleven, etc.)

http://www.nytimes.com/2009/08/18/technology/18card.html?hp

How Hackers Snatch Real-Time Security ID Numbers
http://bits.blogs.nytimes.com/2009/08/20/how-hackers-snatch-real-time-security-id-numbers/#more-17385

European Cyber-Gangs Target Small U.S. Firms, Group Says

http://www.washingtonpost.com/wp-dyn/content/article/2009/08/24/AR2009082402272.html?nav=hcmodule