The Franchise Valuations Reporter

404 Park Avenue South, 16th Floor, NY, NY 10016 Volume 1, Issue 9 – Oct/Nov 2009
212.689.0400 / Bruce@FranchiseValuations.com

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 email reporter you may unsubscribe below.

Nexus Notes

California Taxing Franchise Royalties – Update

As we reported in our last issue the California Franchise Tax Board has recently been contacting non-resident franchisors telling them they must either register and file income tax returns or have their California franchisees withhold 7 percent of royalty payments. We provided an example showing how much cheaper it is to register than be subject to withholding (See Franchise Valuations Reporter Volume 1 Issue 8).

Since then the IFA has advised that franchisors may be able to contest nexus based on the *Rainier Brewing Co* case (210 P.2d 233). In our opinion to make such argument would be most unwise. The case is from 1949 - 60 years ago - and specifically notes that other states involved were not seeking to tax the royalties at issue. As precedent it is monstrously outdated and, in our opinion, its fact pattern offers no protection against a nexus finding in the 21st century.

Daubert Decisions

In *MDG International v. GMAC Australian Gold, Inc.*, 2009 WL 1916728 (S.D. Ind.) (June 29, 2009), a District Court held that although the expert had generally commendable qualifications[1] to prepare a business valuation, nonetheless in a warning to counsel against stacking the deck, disqualified him from testifying because his opinions "rely on incomplete and inaccurate 'cherry-picked' facts." His opinions were excluded because he relied solely on the very limited and selected information provided to him by counsel for MDG; and because he did not review the record in preparing his report. Moral of the story: litigators must give their experts a complete record. Also it shows how extensive and expensive the services of such experts will be when they are obligated to review the entirety of bloated discovery files.

Litigation counsel are well advised to review **Ten ways lawyers kill their own experts** http://www.abanet.org/media/youraba/200910/article02.html

[1] MDG used the services of Professor James Wahlen, Ph.D., a professor of accounting and the chairman of the Master's of Business Administration program at the Indiana University Kelley School of Business.

CyberCrime

As of the time of this writing, the Red Flags Rule is scheduled to come into effect November 1, 2009

Part 2: The Red Flags Rule and Data Security

The Red Flags Rule ("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. A Red Flag is defined as a pattern, practice or specific activity that indicates the possible existence of identity theft. Part 1 of this report, in the **September issue** of *The Franchise Valuations Reporter*, discussed how franchisors and franchisees may be subject to the Rule under the FTC's definitions of "creditors" and "covered accounts."

In Part 2 we cover the requirements for implementing a prevention program to detect Red Flags or the warning signs of the use of stolen identities. Then we discuss some data security best practices as they apply to franchising.

As we noted in Part 1, some franchisors 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 "picks up where data security leaves off," according to Manas Mohapatra, an attorney with the FTC. (See Colleen McCarthy, "FTC's Red Flags May Color Some Surprised," BusinessInsurance.com, July 26, 2009.) It is about preventing *the use of* false identities, not about preventing identity theft in the first place. 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.

Once an organization determines that it is subject to the Rule, it must develop and implement a written Identity Theft Prevention Program, and ensure that appropriate staff members are trained. If the company outsources any of its operations that are covered by the Rule, the Program must also address how contractors' compliance will be monitored.

Four Steps of Program Design

Step 1: IDENTIFICATION. The Program must spell out ways to identify red flags that are likely to come up in day-to-day operations. The FTC gives "illustrative examples" within five common categories:

- Alerts, notifications, or warnings from a consumer reporting agency, for example, a notice of a credit freeze or address discrepancy from a credit reporting agency;
- Suspicious documents, such as those presented by a person who doesn't resemble the photo or match the physical description;
- Suspicious personally identifying information, such as an address, telephone number, or social security number that's been used by other people opening accounts;
- Unusual use of – or suspicious activity relating to – a covered account, such as

an account that's been inactive for a long time suddenly being used again; and
- Notices from customers, victims of identity theft, law enforcement authorities, or other businesses that an account has been used fraudulently.

Other examples may be found in the Federal Register at page 63767.

Step 2: DETECTION. The program must state how employees will **detect** such warning signs. Depending on the kinds of red flag warnings, this may include training employees in ways to verify someone's identity or creating a centralized log of identity theft notices.

Step 3: RESPONSE. A company's Procedures Manual MUST address how to **respond** to and mitigate the harm from identity theft. If a warning sign is detected, the appropriate response depends upon the degree of risk posed. In its Guidelines at p. 63773, the FTC offers a range of appropriate responses, including:
- monitoring a covered account for evidence of identity theft;
- contacting the customer;
- changing passwords, security codes, or other ways to access a covered account;
- closing an existing account;
- reopening an account with a new account number;
- not opening a new account;
- not trying to collect on an account or not selling an account to a debt collector;
- notifying law enforcement; or
- determining that no response is warranted under the particular circumstances;.

Step 4: UPDATES. The Program must 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.

Administration

The initial Program must be approved by the organization's board of directors, or if there is no board, by a senior-level employee. A senior manager must be designated as the person responsible for the Program and he or she should report at least annually to the board of directors or a designated senior manager. The report should evaluate how effective the Program has been in addressing the risk of identity theft; how the company is monitoring the practices of its service providers; significant incidents of identity theft and the company's response; and recommendations for major changes to the Program.

As noted above, enforcement of the Rule is scheduled to begin November 1, 2009. Failure to comply could result in civil fines up to $3,500 per incident.

Best Data Security Practices

As we have previously reported, the Red Flags Rule is meant to thwart the use of stolen identities by customers who try to access existing credit accounts or to open new ones while posing as someone else. Prevention of the theft of personally identifiable information in the first place is another story, subject to regulations under data privacy and security laws such as HIPAA, the Gramm-Leach-Bliley Act (GLBA) and the U.S.A. Patriot Act, as well as industry standards such as PCI DSS. These laws and standards require that companies that collect and store personal consumer information implement integrated theft prevention programs. See, e.g.**,**"Cyber Crime and Cyber Security: A White Paper for Franchisors, Licensors, and Others," prepared by the staff of Franchise Technology Risk Management.

The Importance of Written Policies.

At the heart of any data security program are the policies and procedures that govern how the information security process is implemented. As an indication of their importance, the term "policies and procedures" is found at least 17 times in the actual text of FACTA. Beyond complying with the Red Flags Rule, companies should have policies in place with respect to data protection, data retention, data destruction, privacy, and disclaimers to customers. And, if a security breach occurs, the company should expect, and be prepared for, a regulatory investigation during which the company will have to show that its policies were well documented, updated as business processes changed and observed. If not, the company risks significant fines, agency oversight, or worse. The policies must be more than mere window dressing; failure to conform to a company's own stated, internal policies may be worse than having no policies at all.

What kinds of policies should be included in a security policy manual? According to Henfree Chan, co-founder of Franchise Technology Risk Management (FTRM), an effective data security plan should address, at a minimum: 1) physical security, 2) electronic access controls, 3) intrusion detection, 4) incident response planning, and 5) employee training.

Conclusion

Reaction to the Red Flags Rule has been mostly negative within the franchise and legal communities, focusing on the burdens such a regulation creates rather than on the benefits. While it may turn out that relatively few franchise systems are actually subject to the Rule, the increased attention in the news media to the prevalence of identity theft may have a positive outcome by acting as a wake-up call.

Designing a security plan begins with a vulnerability assessment to determine where the organization might experience attacks. While there are some off-the-shelf programs that purport to do such assessments, the FTC suggests having independent professionals conduct a full-scale security audit. Most franchise companies are totally unaware of the vulnerabilities in their technology infrastructure. Penetration testing is the only effective way to identify the flaws that might be exploited by intruders. Using the latest hacking techniques, a penetration test probes the vulnerabilities of a company's infrastructure, web applications and wireless networks from the perspective of an attacker.

Considering the costs of a security breach – to a company's reputation, in defending against lawsuits and regulatory investigations and from the interruption of business – taking steps to safeguard sensitive personal information about employees and customers is simply good business.

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.

MORE REASONS TO BE FRIGHTENED!
Links to Recent Articles on Cyber-Crime

Banking Trojan steals money from under your nose

http://news.cnet.com/8301-27080_3-10363836-245.html

Credit Card Skimming Survey: What's Your Magstripe Worth?
http://www.wired.com/threatlevel/2009/10/florida_skimming/

FBI snags 100 people in global identity-theft scheme
http://latimesblogs.latimes.com/lanow/2009/10/more-than-100-people-have-been-arrested-this-morning-in-connection-with-a-global-identity-theft-ring-agents-with-the-federal-1.html

Scammers Hijack Accounts of Second Law Firm—Fish & Richardson
http://www.abajournal.com/weekly/another_law_firm--fish_richardsonsays_scammers_hijacked_its_accounts