FRANCHISING WORLD®

TECHNOLOGY

Why Franchisors Need to be Concerned about Hacking

Data security breaches and FTC enforcement powers could ignite a "giant cauldron of litigation."

BY PETER R. TAFFAE

Many franchisors still believe that only Fortune 500 companies are susceptible to cyber hacking, even though the National Cyber Security Alliance reported 20 percent of companies fall victim to a cybercrime and of those 60 percent go out of business within six months.

At the International Franchise Association convention in Las Vegas earlier this year, the general feeling was the franchisor is not accountable for the cyber problems of the franchisees. Even though most franchisors suggest or require certain POS software as well as hardware be purchased by the franchisees, the general conscientious was a lack of urgency or outright denial. This thinking causes serious problems. Unless the franchisor's accounting department is using abacuses and pencils it is a matter of when, not if there will be a data security breach.

The Federal Trade Commission is the federal agency that regulates franchising. Its Franchise Rule applies everywhere in the United States. The FTC also, historically, has also been the most active federal regulator in data privacy/security. The agency's broad enforcement action is based on privacy violations arising from (alleged) unfair or deceptive practices that allow for consumers' private information to be at risk. The FTC has brought hundreds of cases against companies it feels have violated consumers' privacy.

(Continued on page 94)

(Continued from page 93)

Each day we read about data security breaches, challenges and its effects of the viability of the victimized company. Data security is big news. As is the FTC's enforcement powers. Put them together and expect a gigantic cauldron of litigation.

NEW REALITIES

Franchisors' cyber complacency just got real. It's now on top of the "to do" list of prudent franchisors due to a significant case brought by the FTC against Wyndham Worldwide Corp. After three separate unauthorized (hacker) intrusions within two years (2008- 2009). The FTC sued Wyndham in federal court alleging that the company failed to employ "reasonable and appropriate" cyber security procedures. The agency argued that Wyndham had inadequate data (cyber) security policies and procedures in place, and pointed specifically to the duties Wyndham had over its franchisees, among other allegations.

In March, the U.S. Court of Appeals for the Third Circuit held oral arguments on Wyndham's appeal. The outcome of this case, no matter who is victorious, will certainly change the franchisor cyber regulatory landscape extensively. Over the years, the FTC has been developing substantial body of jurisprudence involving consumer private data. Many believe no matter what the outcome, the court's opinion will have wide ranging consequences for franchisors.

WHAT'S THE FUTURE HOLD?

If the FTC prevails, the verdict may propel increased enforcement. Franchisors' standard of care over its franchisees will very likely heighten. With this new "undoubting authority" we can expect increased frequency and severity of consumer privacy enforcement. Do the directors' and officers' of the franchisor have a new threat with which they must be concerned? Like the cyber breaches at Target, Home Depot, and others, investors' litigation typically follows cyber breaches. It would not be a surprise to see unaffected franchisees bringing litigation against directs or officers alleging mismanagement resulting in harm to the brand. With a rare exception, securing broad D&O/ E&O insurance together with vicarious liability protection is near impossible to obtain. Ideally the franchisor should have the D&O and Franchisor Malpractice (E&O) with the same insurance company to avoid unnecessary problems. Another real concern for franchisors should be the cyber insurance products available today never taken into consideration the FTC/ Wyndham verdict. The current cyber policies available in the market are not adequate for a post-Wyndham cyber world.

If Wyndham prevails the irony is that what comes in to fill the government oversight, could be less favorable to franchisors. Although the general conscious is the FTC enforcement power will be confirmed; if Wyndham succeeds the outcome could be bad news for the franchise industry. Congress would most likely rework legislation that could give the FTC or other federal agencies even broader regulatory powers. At the same time, many states will see this as a time to enact their own consumer data laws. Do franchisors (all but the largest) have the financial bandwidth to survive these new realities? Will they need to modify their FDDs to adapt to this new reality?

PROACTIVE STEPS

Franchisors must take a proactive approach to ever increasing risks of cyber security. "Buckle your seat belts," says Jeffrey Wolf, a litigation partner in the Phoenix office of Quarles & Brady. According to Wolf, "in-house counsel and board members should be preparing to implement a risk security program while also understanding their company's insurance coverage".

A comprehensive approach would include:

VENDER MANAGEMENT

The Target breach arose out of their HVAC vendor lack of security that allowed a hacker to penetrate the Target data. A closer look at the vendor contract is a wake up call to the importance of third party contractual relationship. A wise consideration would include obligation post relationship.

POST BREACH

Waiting until a breach occurs to have an action plan will not suffice. Quite to the contrary, it will only compound the problem. It is not different than having annual fire or earthquake preparedness drills. Franchisors should have a plan and routinely practice it. This should include having an appropriate set of necessary steps for public relations, media responses, forensic exports, date security, and other key crisis management programs Insurance

Having the correct insurance plays an important part. It is important to seek professionals who have the insurance expertise and franchise industry knowledge. One size does not fit all. The correct policy should address the needs of the franchisor while taking into account network issues that also impact the franchisees operations.

Remember the Target vender gateway? Franchisors have sustainably more gateways (franchisees). Many, but not all, insurance companies offer pre-approved cyber security, forensic and public relations experts. No one will argue that the cyber landscape is liquid and is consistently changing. Be sure to secure a state of the art policy. ■

Peter R. Taffae is managing director of Franchise Perils (descriptor). Find him at fransocial.franchise.org