LJN'S
FRANCHISING BUSINESS & LAW ALERT®

LAW JOURNAL NEWSLETTERS

An incisivemedia publication

Volume 15, Number 6 • March 2009

Preventing Conflicts Between Secured Creditors and Franchisors

By Craig R. Tractenberg

Lenders, franchisees, and franchisors all have a concern in preventing conflicts between their respective interests. The Uniform Commercial Code ("UCC") was amended to strike a balance among the parties. However, the recent credit crisis has demonstrated that the UCC is only the starting point for the analysis. Some counsel advocate that franchisors should attempt to perfect their interests as secured creditors. The realities of franchising require closer study of whether this is advisable and whether it is better to negotiate superior arrangements.

The UCC grants secured creditors certain "rights, obligations and remedies" against third parties, such as the borrower, other lenders, tax creditors, and the franchisor. In UCC parlance, the "secured creditor" (typically a lender) takes a "security interest" (a lien) in "collateral" (typically assets of the franchisee), and that interest has priority over the conflicting claims of third parties (other creditors and the franchisor). The secured interest is "authenticated" by a "security agreement," which is the contract between the secured creditor and the debtor. The security agreement describes the collateral that secures the debt, and the rights and remedies of the secured creditor. Theoretically, the security agreement no longer

continued on page 6

Franchise Companies vs. Hackers

Twenty Questions on Cybercrime

By Henfree Chan and Bruce S. Schaeffer

The 21st century is clearly the age of cybercrime, and franchise companies should be especially concerned because, simplistically, there are only two types of computer systems: those that have been hacked, and those that will be hacked. Franchise companies are uniquely vulnerable in two areas because they possess massive collections of personally identifiable information ("PII"), and they have substantial asset bases of intangible property. Both the PII and the intangible assets can be easily copied without leaving the premises. Any transaction involving a card with a magnetic strip involves risk, and any franchise company's computer system designed to allow access to multiple users (such as franchisees, vendors, suppliers, etc.) poses an enormous risk of being penetrated. All companies using e-mail or the Internet are vulnerable; firewalls offer no protection once a hacker has infiltrated.

And things are going to get worse. Speaking to the BBC for a report on technology, Mikko Hypponen, chief research officer at F-Secure, an IT security firm based in Helsinki, Finland, said last year, "Crime tends to rise when you have more unemployment. If you look, in general, where the attacks are coming from you can find social reasons behind them." Experts at the 2009 World Economic Forum in Davos, Switzerland, called for a new system to tackle well-organized gangs of cybercriminals, and they claimed that online theft costs $1 trillion a year, that the number of attacks is rising sharply, and that too many people do not know how to protect themselves.

Even if you can protect your system from outsiders, a franchise company can still be easily betrayed from within. "The damage that insiders can do should not be underestimated. It can take just a few minutes for an entire database that has taken years to build to be copied to a CD or USB stick," said Adam Bosnian, a spokesman for Newton, MA-based Cyber-Ark, a developer of "digital vaults" for securing electronic information.

continued on page 2

In This Issue

Cybercrime

continued from page 1

"With a faltering economy, companies need to be especially vigilant about protecting their most sensitive data against nervous or disgruntled employees," Bosnian told the BBC. A prime example of this is the recent case of mortgage giant Fannie Mae, which narrowly avoided a software time bomb set to destroy all data on its computers. Federal authorities allege that a disgruntled contractor embedded a malicious code in Fannie's system, set to go into effect on all 4,000 of the company's servers months after he was gone. The code was tucked at the end of a legitimate software program scheduled to run each morning and was discovered only by chance by another Fannie technician.

According to the Identity Theft Resource Center, based in San Diego, breaches were up more than 25% in 2008 and affected more than 35.7 million people. "This may be reflective of the economy, or the fact that there are more organized crime rings going after company information using insiders," said Linda Foley, the Center's co-founder. "As companies become more stringent with protecting against hackers, insider theft is becoming more prevalent."

Accordingly, a franchise company must evaluate its risk to determine and implement appropriate policies and procedures. The authors have formulated a "Chan Scale of Cyber In-Security©," which can provide franchise companies a framework for considering the potential harm that can be caused:

1 Chan — Low risk. Hacker has gained entry to system, but minimally. Minor risk of business disruption, but access can aid attackers in gathering information and planning future attacks.

2 Chans — Medium. "Malware" has been implanted in the company's network that could cause malfunctions and mischief. Significant risk of a business disruption that could result in financial loss and/or damage of good-will.

3 Chans — Medium-to-high. Using sniffers or other equipment, hackers have obtained PII from point-of-sale systems. Significant risk of business disruption that could create financial loss and/or damage of goodwill.

4 Chans — High. Often an inside job in which data are stolen by a disgruntled employee. Serious risk of business disruption that would result in financial loss and damage of goodwill; customers' PII may be vulnerable, as well as company's confidential information and financial information.

5 Chans — Critical. Hackers have breached system and can access PII as well as the company's financial information and confidential information. Severe risk of business disruption, financial loss, and damage of goodwill. System, applications, and database have been compromised.

In light of such exposure, franchise companies may have to reach out to members of the organization with diverse areas of expertise, including legal, technical, risk management, finance, and crisis management. Here are 20 questions about cybersecurity that need to be answered. (For an exhaustive review of this subject, *see The Financial Impact of Cyber Risk*, published jointly in 2008 by the American National Standards Institute and the Internet Security Alliance. The report provided the basis for many of the questions herein.)

continued on page 3

Henfree Chan and **Bruce S. Schaeffer** are co-founders of Franchise Technology Risk Management (www.FTRM.biz), a unit of Franchise Valuations, Ltd. in New York City. Chan is a senior information security professional, formerly with Deutsche Bank and Goldman Sachs. Schaeffer is a franchise attorney specializing in valuations, damages, and tax issues of franchise operations. He can be reached at 212-689-0400 or Bruce@FTRM.biz.

FRANCHISING

BUSINESS & LAW ALERT®

LJN'S Franchising Business & Law Alert® (ISSN 1079-6339) is published by Law Journal Newsletters, a division of Incisve Media.
Telephone: (877) 256-2472
Editorial e-mail: julie.gromer@incisivemedia.com
Circulation e-mail: customercare@incisivemedia.com
Reprints e-mail: reprintscustomerservice@incisivemedia.com

LJN's Franchising Business & Law Alert 023145
Periodicals Postage Paid at Philadelphia, PA
POSTMASTER: Send address changes to:
Incisive Media
120 Broadway, New York, NY 10271

Published Monthly by:
Law Journal Newsletters
1617 JFK Boulevard, Suite 1750, Philadelphia, Pa 19103
www.ljnonline.com

incisivemedia

Cybercrime

continued from page 2

General

1) What is the definition of cyber security?

Answer: The protection of any computer system, software program, and data against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. Cyber-attacks can come from internal networks, the Internet, or other private or public systems.

2) Is cybercrime on the rise?

Answer: On average, there has been a reported cybersecurity event every single day since 2006. Thefts of PII have been reported regularly in the media, but other types of attacks against public and private entities, though much less often reported, have resulted in data destruction, down time, etc.

3) What financial exposure attaches to cybercrimes?

Answer: Major liability may be incurred from individual litigation, class litigation, regulatory investigation, contract dispute, loss of customers, reputation damage, data theft, denial of service, cyber terrorism, cyber extortion, and fraud.

Questions for the Company's Lawyer

4) Has the company's cyber liability been analyzed?

Answer: Potential liabilities may relate to the information kept by the company, its vendors, or third parties.

5) Has cyber protection been built into contracts with vendors?

Answer: Wherever possible, vendors (especially applications vendors) should be required to warrant that company data are appropriately protected and should be required to indemnify the company for losses arising from cybersecurity breaches that are the fault of the vendor. Furthermore, contracts should require that vendors have network security insurance, which shifts the financial burden for losses to the insurer. The other benefit of insurance is, typically, it indicates that a third party (the insurer) has thoroughly evaluated the vendor's cybersecurity systems.

6) Has the cyber risk to trade secrets and other IP been assessed?

Answer: Confidential operating manuals, trade secrets, and other intellectual property are the mainstays of franchise systems. Because these usually are held in electronic or digital form, they are easily subject to misappropriation through a cyber attack. Unlike the theft of physical assets, a theft of digital assets leaves the stolen asset behind — which makes the theft much more difficult to discover — so that without penetration testing and proper monitoring, a franchise company may not even know it's been compromised.

7) What can be done to mitigate cyber risk, and how often should a franchise company conduct a cyber analysis or cyber audit?

Answer: Performing comprehensive reviews of all systems and system logs at least quarterly is essential. Franchise companies also must perform a legal audit of all applicable regulations, vendor contracts, internal procedures, and policies to deal with potential thefts of PII. In the event of a breach, the audit trail will help to keep the costs of litigation under control.

8) Has the company analyzed what regulations (federal, state, local, and global) exist with respect to cyber data, and whether or not the company is in compliance?

Answer: Some statutes addressing liability include:

- Communications Act of 1934, updated in 1996;
- Computer Fraud and Abuse Act of 1984;
- Computer Security Act of 1987;
- Economic Espionage Act of 1996;
- Electronic Communications Privacy Act of 1986;
- Federal Privacy Act of 1974
- Health Insurance Portability and Accountability Act of 1996;
- National Information Infrastructure Protection Act of 1996; and
- U.S.A. Patriot Act of 2001.

In the 21st century, a company cannot expect to claim ignorance of applicable regulations and get away with it.

9) How is compliance monitored on an ongoing basis?

Answer: In the event of a security breach, a company must be able to demonstrate that it had reasonable processes in place to ensure compliance with regulations, including access controls and visible audit trails. Without these processes, a company's potential liability increases.

10) Does the company have policies in place with respect to data retention, data destruction, privacy policies, and disclaimers to customers?

Answer: If a security breach occurs, the company should expect a regulatory investigation. Unless the company is able to show that its policies were well documented, up-to-date, and observed, it will risk 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.

Questions for the Technology Team

11) Is there a companywide compendium or directory of what regulated data the company has, where it exists, and what format it's in?

Answer: If there is, it must be regularly reviewed. If the directory doesn't exist, it must be created.

12) How vulnerable are the confidentiality, integrity, and availability of the company's data systems?

Answer: Confidential information includes anything a company wants to keep out of the hands of competitors and the public. Examples include recipes, operations manuals, customer lists, and personal data about executives and employees. There must be a plan in place to keep this information

continued on page 4

Cybercrime

continued from page 3

secure, and it is also important to maintain the integrity (*i.e.*, the accuracy) of the company's records and the availability of systems to keep the business running (*e.g.*, to avoid or contain a denial-of-service attack). The cost of downtime can be devastating.

13) Does the company have physical security controls at each of its sites (data center, home office, franchisees, or other sites)?

Answer: Physical security, which is relatively low-tech, can easily be overlooked in the process of protecting digital assets. Nonetheless, good cybersecurity practices must include appropriate barriers to the accidental or malicious access to vital systems by unauthorized persons, such as keeping them away from company computers.

14) How often does the company re-evaluate its technical exposure?

Answer: Although a security plan might be sufficient at any one point in time, new techniques for exploiting vulnerabilities are always being developed by hackers. In order to provide long-term protection, the franchise must have personnel and processes in place to maintain current about new types of threats and must engage in regular periodic internal penetration and security testing.

Questions for the Crisis Management Team

15) Has the company prepared incident response and business continuity plans based on a full understanding of the potential financial impact of a crisis? And has the company conducted "fire drills" to see if its plans work?

Answer: Unfortunately, there is no way to ensure protection against cyber attacks 100% of the time. This makes careful planning and flawless execution of a crisis management plan a necessity. The company should conduct mock drills on a regular basis, evaluate the performance of all components, and make adjustments to remedy any deficiencies.

16) If the company's computer system is penetrated, does the company's crisis communications plan include provisions to advise all necessary parties about the situation? If there's a cybersecurity event involving PII, does the company have an existing set of procedures to identify who must be notified and how to do it?

Answer: Many regulators demand prompt notification of individuals affected by a data security breach. The company must have protocols in place to communicate the required details to the regulators and the affected populations quickly and accurately.

17) Does the company have a budget and reserves to account for a cyber event? Is it reflected in the company's financials?

Answer: The expense of dealing with a cybersecurity event can come as a shock. According to some studies, the average cost of basic notification for a large data breach can be $1-$2 per customer record and may reach $3-$6 if call center services are required. According to research from the Ponemon Institute, a security research firm, the cost of data breaches in 2007 was $202 per compromised record.

Questions for the Franchise Executive in Charge of Insurance

18) Does the company have insurance to cover cyber events? Is there a provision regarding PII?

Answer: This must be carefully reviewed with the company's P&C carrier because most policies focus on damage to tangible assets only.

19) Does the policy cover identity theft?

Answer: Many policies do, and many identity theft risk-management services include personal identity theft insurance as part of the service.

20) Will the franchise company's directors and officers face increased potential liability if they don't get cyber insurance?

Answer: Failure to obtain insurance against financial loss may be grounds for a management liability suit by shareholders. Yet, most D&O policies have an exclusion for a "failure to obtain insurance" claim.

Conclusion

Any franchise company that doesn't recognize the enormity of its potential exposure and liability to cybercrime is delusional. All franchise companies must, at a minimum, learn to search for and keep track of vulnerabilities; hold vendors responsible for supplying patches or fixes in a timely manner; check user access to software programs; and mandate the use of passwords by all authorized employees.

Most importantly, franchise companies must conduct penetration testing of all corporate networks and Internet-facing applications to see, among other things, if there have been penetrations, if there is any unapproved software installed on peer-to-peer file-sharing software, or if anything else can compromise the company's confidential data. These prophylactic reviews must be done regularly and done by security professionals. IT departments are usually well-informed about applications and networks, but in-house IT staff might not be as current about data protection and information security.

Franchise companies are well advised to start evaluating their technology risk as soon as possible before the hackers beat them to it. *The Financial Impact of Cyber Risk* report concluded, "An organization that is unprepared to avert or manage a data breach can suffer severe financial losses and irreparable damage to its reputation and customer base. Conversely, when an organization is prepared and responds skillfully to a cyber threat, the crisis can go down … as an event that cements customer loyalty and a positive brand image."

—❖—

COURT WATCH

By Cynthia M. Klaus and Meredith A. Bauer

CA District Court Confirms Unconscionability of Arbitration Provision

Franchisors have long been watching the California courts and their interpretation of arbitration provisions under California law. Since the *Nagrampa v. MailCoups, Inc.* decision in 2006, which found procedural and substantive unconscionability in a relatively standard franchise agreement arbitration provision, a real concern exists as to whether such arbitration provisions can be enforced in California.

The Northern District of California is the most recent court to weigh-in on the enforceability of arbitration provisions contained in franchise agreements under California law. In *Bencharsky v. Cottman Transmission Systems, LLC*, Bus. Franchise Guide, 14,045 (CCH) (D.C. Cal. 2008), the court determined that both procedural and substantive unconscionability existed in an arbitration provision, partly due to a lack of mutuality as to the availability of equitable relief for the franchisor and the franchisee.

In this case, the franchisor filed a demand for arbitration against one of its automotive repair franchisees, alleging unpaid franchise fees. The franchisor relied on a provision of the franchise agreement which stated that the parties should attempt to resolve all disputes in arbitration, but also reserved its right to obtain equitable relief in court. The franchisee then filed suit in court, alleging in part, breach of contract and violation of the California Franchise Investment Law ("CFIL"). The franchisor then moved to compel arbitration of the franchisee's claims.

Cynthia M. Klaus is a shareholder at Larkin Hoffman Daly & Lindgren Ltd. in Minneapolis. She can be contacted at cklaus@larkinhoffman.com or 952-896-3392. **Meredith A. Bauer** is an associate at the firm. She can be contacted at mbauer@larkinhoffman.com or 952-896-3263.

Issue of Arbitrability. The court initially tackled the issue of whether an arbitrator, or the court itself, was the proper authority to determine whether the arbitration clause was enforceable. The court used the "crux of the complaint" test, meaning that when the "crux of the complaint" challenges only the arbitration provision and not the invalidity of the contract as a whole, it is up to the court to decide whether the arbitration provision is enforceable. In comparison, the issue of arbitrability is an issue for an arbitrator when the "crux of the complaint" is that the agreement as a whole is void and unenforceable.

Here, the court found that the "crux of the complaint" was that the arbitration provision itself was invalid. Thus, the plaintiff was seeking a determination as to the validity of the arbitration clause, and it was up to the court to decide the arbitrability issue. Interestingly, the fact that the plaintiff also sought rescission of the contract as a whole was not determinative in deciding the "crux of the complaint" test.

Choice of Law. The franchisor argued that the enforceability of the arbitration provision should be decided under Pennsylvania law, which was designated as the governing law in the franchise agreement. Even though the franchise agreement had been signed in Pennsylvania and the franchisor's home office was located in Pennsylvania (and thus a substantial relation to Pennsylvania existed), the court found that Pennsylvania law was contrary to the fundamental policy of the CFIL. To support this finding, the court pointed out two instances in which California law provided greater protection to franchisees than Pennsylvania law: 1) the CFIL allows franchisees to bring actions against individual defendants without requiring franchisees to pierce the corporate veil; and 2) California common law allows a franchisee to establish fraud if the franchisor provides information in a misleading manner, as opposed to Pennsylvania common law, which provides a defense to franchisors if the communication was factual. Therefore, the court rendered the choice-of-law provision in the franchise agreement unenforceable and applied California law to the interpretation of the arbitration clause.

Procedural Unconscionability. The court went on to find both procedural and substantive unconscionability in the arbitration provision of the franchise agreement and the factual circumstances surrounding the case, both of which must be present in order to render a provision of an agreement unenforceable. Procedural unconscionability was established based on the unequal bargaining power between the franchisor and franchisee. Under this interpretation, almost all franchise agreements would be tainted with procedural unconscionability due to the nature of the franchise relationship. The court did point out several mitigating factors, including that the franchisee had consulted with an attorney prior to signing the franchise agreement, that the arbitration clause was the same size font as the rest of the agreement, and that the words "mandatory arbitration" appeared as a distinct heading in the agreement; but these did not overcome the franchisee's claim of procedural unconscionability.

Substantive Unconscionability. The court found substantive unconscionability in the following provisions of the arbitration clause:

- *Right to obtain equitable relief in court.* The franchisor reserved the right to pursue equitable or injunctive relief in the event the franchisee breached the agreement. Rejecting the franchisor's argument that it needed access to the courts in order to protect its trademarks, the court found the lack of mutuality in this provision rendered it unconscionable, as the franchisor was the party with the most bargaining power in the relationship.
- *Waiver of statutory rights.* The court then found that two

continued on page 6

Court Watch

continued from page 5

clauses in the arbitration provision limited rights that would otherwise be available to the franchisee under the CFIL: A clause providing for a shorter statute of limitations than that provided by statute was unconscionable; and a clause that provided that no punitive or exemplary damages could be awarded by the arbitrator (therefore limiting the type of recovery the franchisee could otherwise obtain under the statute). As the court stated in its decision, the arbitration agreement cannot be used as a mechanism for the franchisee to waive statutory rights.

- *Arbitrator's authority.* Finally, the court found that a provision stating that the arbitrator has no authority to alter or modify a provision of the franchise agreement was unconscionable, for the same reasons as stated above.

Just as interesting as the interpretation of the enforceability of the arbitration provision itself is the court's determination as to the franchisee's available remedies. Although the court found three circumstances of substantive unconscionability, as well as procedural unconscionability, the court ignored the franchisee's request that the entire arbitration provision be invalidated. Instead, the court found that the unconscionable provisions were severable from the remainder of the arbitration clause, and although each unconscionable provision itself was invalid, the dispute would otherwise go to arbitration.

Based on this decision, franchisors may want to consider modifying their franchise agreements if they are used in California. Many franchise agreements provide for arbitration, but allow the franchisor the option to seek equitable relief in court. If such a provision does not give the franchisee this same right, however, the franchisor risks a finding that the clause lacks mutuality, and is therefore unconscionable and unenforceable. Because the provision is severable from the remainder of the franchise agreement, the franchisor risks losing its access to the courts to obtain injunctive relief.

Lease of Franchised Location to a Competitor

The interesting factual circumstance in *Gallagher's NYC Steakhouse Franchising Inc. v. 1020 15th St., Inc. et. al*, Bus. Franchise Guide, 14,035 (CCH) (D.C. Col. 2008), highlights the importance of the specific wording of noncompetition provisions often contained in franchise agreements. After a steak restaurant franchisee breached its franchise agreement, the franchisor obtained a preliminary injunction prohibiting the franchisee from operating a restaurant or other steakhouse at the former franchised location, in accordance with the noncompete provision contained in the franchise agreement. Subsequently, the franchisee leased the former franchised location to a competitor, who opened a competitive steak restaurant in the same space.

The competitor had been the chef at the former franchised restaurant and was a business associate of the franchisee. Not only did the franchisee lease the space to the competitor, but the franchisee also assisted the competitor in forming an entity to operate the new restaurant, obtaining a liquor license, and transferring phone numbers. The new restaurant operated under almost an identical menu as the former franchise.

The franchisor brought suit for violation of the preliminary injunction and for violation of the franchisee's noncompete provision in the franchise agreement. The provision in question provided that the franchisee could not, directly or indirectly, engage in any other steakhouse restaurant business within a certain territory. The franchisor argued that the former franchisee was indirectly doing business at the former franchised location, and was "working in concert" with the competitor to violate the noncompete provision.

The court, interpreting Florida law, decided that because the franchisee did not have operational control or a right to profit in the competitive business, he was not directly or indirectly doing business at the former franchised location in violation of the noncompete provision or the preliminary injunction. Additionally, even though the franchisee would benefit from the operation of the restaurant through rent payments, this is not enough to show that the former franchisee was "in active concert or participation" with the competitive party. Also, the assistance provided by the former franchisee to the competitor was of a brief duration, and the court found that the former franchisee had a legitimate business reason for this assistance in that the franchisee needed to ensure the proper transfer of licenses and documents to the competitor.

Interestingly, the court noted that to guard against this situation, the franchisor should have included language in its franchise agreement prohibiting the franchisee from leasing the franchised location to a competitor.

—❖—

Secured Creditors

continued from page 1

needs to be in writing as long as it is authenticated by click license or even an audio recording (if it is authenticated). Merely having a security interest in collateral is insufficient for the secured creditor to gain much advantage over other conflicting interests.

A secured creditor gains its primary advantages by filing a UCC-1 financing statement. This filing gives notice to the world of the secured creditor's interest and describes the collateral subject to the security interest. The location for filing the UCC-1 is contained in the UCC, and it usually must be filed in the state of incorporation of the debtor, which is not necessarily the state where the debtor operates. A secured creditor seeking to "perfect" its security interest must search the records to assure itself that its filing is first or will have priority over earlier security interests. Security interests that are perfected first have priority over all later liens, but for a

continued on page 7

Secured Creditors

continued from page 6

few exceptions. One exception is for "purchase-money security interests," which grant a priority to the lender that loaned the money to purchase a particular item of collateral upon notice to the earlier perfected secured creditor.

The lender that perfects its security interest in the franchisee's collateral has a lending base that provides confidence for the credit that is being extended. The collateral may include the franchisee's franchise agreement, inventory, contracts, intangibles, receivables, furniture, computers, customer lists, and virtually anything of value. However, most of this collateral has little value unless the business is operating or is sold as a going concern. The lender dreads the day when it might be required to realize on the collateral because the business may not be operating, and the lender will need to fight with the franchisor about how the lender should be paid in these circumstances. For example, the lender may want the franchised business sold to anyone for any amount so that the lender can obtain some proceeds for the good will of the business. The franchisor may want the business to be closed rather than to be operated by a marginal transferee.

Impact of UCC §9-408(A)

The UCC was amended to provide a balance between the needs of the franchisor and the secured lender. In effect, UCC §9-408 subordinates the interests of the lender to the franchisor. In accordance with §9-408(a) of the UCC, the rights of a secured creditor in a franchise agreement as collateral are subject to the limitations that it: a) is not enforceable against the franchisor; b) does not impose a duty or obligation on the franchisor; c) does not require the franchisor to recognize the security interest, pay, or render performance to the lender, or to accept payment or performance from the lender; d) does not entitle the lender to use or assign the franchisee's rights under the franchise agreement; and e) does not entitle the lender to use, assign, possess, or have access to any trade secrets or confidential information of the franchisor. This provision applies even if the franchise agreement contains prohibitions against using the franchise agreement as collateral.

The balance struck by the UCC appropriately allows the lender to use the franchise agreement for its collateral base, but gives the lender no rights to sell or assign the franchise agreement for value. The lender can only collect money from the franchisee/debtor as revenues are generated or when the franchised business is sold. The lender cannot operate the franchise or force a sale to a particular buyer, because these rights are limited by the franchise agreement. The maximum force that the lender could use in order to collect its money would be to force a bankruptcy sale or similar state law disposition of the franchised business. This may be the only alternative for the lender to collect its money, and the franchisor may not appreciate having its franchised location on the auction block.

The franchisor under its franchise agreement is entitled to collect all of its money upon sale of the franchise agreement, and based on §9-408, has priority over the lender for all operational aspects of the franchise, including sale and transfer. If the franchised business cannot be sold as a going concern, however, the amount due under the franchise agreement cannot be collected, and the secured lender would collect all of the proceeds, with the franchisor recovering none. Based on this doomsday scenario, some counsel advocate that a franchisor take a security interest in its franchisees as a way to maintain maximum leverage in insolvency disputes. The franchise agreement could be drafted to contain security agreement language, and the franchisor could require the franchisee to sign a UCC-1 at the inception of the relationship and file the UCC-1 to perfect its security interest.

It is prudent for the franchise agreement to contain language granting a security interest in favor of the franchisor, but recording a UCC-1 may conflict with the priority that a lender may demand to finance the franchisee. The franchisor's security interest will interfere with other financing if the franchisor will not subordinate its lien. If no lender is required for the franchise purchase, then filing the UCC-1 to perfect the franchisor's interest assures that the franchisor will obtain the maximum recovery in a liquidation. If a lender is needed, then the franchisor will be required to subordinate its perfected security interest to that of the lender. Even in this subordination arrangement, the lender and the franchisor will remain in conflict because the lender still will want the business to be sold as a going concern to maximize proceeds.

The best solutions to reduce conflict and to maximize recovery may be either an "inter-creditor agreement" or a "remarketing agreement" between the lender and the franchisor. In an inter-creditor agreement, the lender and the franchisor may agree in advance of insolvency to exchange information regarding defaults and cures, engage in collaborative decision-making when defaults occur, and confer on how to handle bankruptcy or reorganization issues, such as voting and plan formulation. For example, the franchisor might negotiate to obtain copies of the lender's default notices at the time they were sent, in exchange for the franchisor standing still in a lender default condition; this could avoid cascading defaults and conflicts between the parties that could lead to the abrupt closure of the franchised business. The inter-creditor agreement is simply a plan on how to proceed if the franchisee defaults to either the lender or the franchisor in order to avoid short-sighted action that frustrates the other parties' rights.

The "remarketing agreement" actually can be a separate agreement or can be included in an inter-creditor agreement. A remarketing agreement allows the franchised business to be sold as a going concern in order to maximize the sale price while

continued on page 8

Craig R. Tractenberg is a partner in the New York City office of Nixon Peabody LLP. He can be contacted at 212-940-3722 or ctractenberg@nixonpeabody.com.

NEWS BRIEFS

SURVEY FINDS LEGAL POSITIONS TOP FRANCHISE COMPENSATION RATES

A new survey by FranData, Inc. pegged median compensation for franchisors' general counsel at $146,000 per year, including bonuses, topping all other managerial-level positions. The Franchise Compensation Report was released in January, and it can be obtained at www.frandata.com.

"Seeing general counsel at the top of the managerial salary range indicates that job functions that had technical qualifications, such as a law degree, bring higher levels of compensation," said Darrell M. Johnson, president and CEO, FranData.

In addition to legal positions, the survey tracked salaries for franchise development, site selection/pre-opening activities, franchisee training, field operations, compliance, and marketing. "This type of survey has never been done before. This is the first time that this information is available about jobs with franchise-specific functions, instead of more broad compensation surveys," said Johnson.

FranData's survey was conducted from September to November 2008. The company mailed surveys to more than 2,000 franchisors, representing more than 3,000 brands. Eighty-seven responses were received with sufficient information to incorporate into the survey; and of those respondents, 11 reported on salaries for legal staff.

Salary data also were collected for professionals who were not managers in each of the seven functional areas. Here, too, average compensation for legal professionals topped the list, at $102,000. However, median compensation showed a different picture, as legal professionals were at about $48,000, which was well below medians for professionals involved in development, operations, marketing, and site selection.

The variation in data reflects that the survey is in its first year and that more responses in the future will improve its accuracy, said Johnson. "There are limits to what we could get in the first year. But we plan to make this an annual survey. Our hope is that as we build on it year after year, more franchisors will understand the importance of contributing to it, and we will be able to become more granular in our analysis," said Johnson.

Johnson said the survey is especially valuable for new franchisors that have a small number of professionals, each of whom is handling several jobs. "As the franchise grows, the people who wore many hats will have to hire people for stand-alone positions in the company," said Johnson. "We are now giving them data points and a framework on which to make judgments about job functions and compensation."

Reflecting the recognition that in any franchise system, people will often have multiple responsibilities, the survey queried franchisors about the areas of functional responsibility for various positions. General counsel reported that about 80% of their time is spent on legal issues, with the balance of their time split between compliance, development, and marketing. Meanwhile, compliance managers reported spending about 10% of their time on legal issues.

Larger franchise systems (251 units or more) reported that they pay their general counsel and legal services staff about 70% more than mid-size systems (51-250 units); there were insufficient responses from small systems to produce data.

FranData also found that compensation for all managers and professionals varied considerably by industry. Table- and full-service restaurants were atop the list, followed by business services and fast-food restaurants. Compensation in retail products and services was at the bottom of the list, at less than half the average of table- and full-service restaurants.

—❖—

Secured Creditors

continued from page 7

the default continues. It may require the lender to force the franchisee to relinquish operation to the franchisor during a marketing period to allow the franchisor to improve operations and sell the business. In exchange, the lender may agree to forbear in foreclosure and to allow the franchisor to collect all of its fees during the marketing period, plus a premium for operating the business, without interference from the lender.

Franchisors and lenders with regular finance programs, particularly with multi-unit lending, should develop an inter-creditor agreement as a vehicle for proposing terms to maximize recoveries and cooperation. An inter-creditor agreement eliminates the need for the franchisor to obtain and perfect a security interest in the franchisee because the parties have agreed about how the rights and remedies of the secured party are subordinated to the franchisor's contractual rights. It provides a game plan that the parties must follow when lender and franchisor would otherwise be acting for their own self interests.

CONCLUSION

In summary, a franchisor has rights and remedies that a secured creditor is not granted under the UCC, but the franchisor, by becoming a competing secured creditor, does not necessarily advance its rights and remedies in a default situation. The inter-creditor agreement and remarketing agreement are alternatives to maximize recoveries and reduce conflicts by cooperation, rather than by litigation.

—❖—