Hospitalitas

News and Views for Your Hospitality and Franchise Business

BAKER DONELSON

EXPAND YOUR EXPECTATIONS℠

Winter 2016

Franchisor Protected from Unfair Competition, Not All Competition

Gene Podesta, 901.577.2213, gpodesta@bakerdonelson.com

The fine line between protecting your system's legitimate interests and trying to eliminate a competitor can be hard to define in advance. With social media so important for consumer businesses, the line is even more difficult to identify in advance. A franchisor should not presume that its branding and trade dress, even its recipes, are protectable or unique just because its documents claim that status.

Continued on page 2

NLRB: Joint Liability Inquiry Can Precede Finding on Merits of Underlying Unfair Labor Practice Charge

Sharonda Childs, 205.244.3837, schilds@bakerdonelson.com

In the latest development in the National Labor Relations Board's ongoing efforts to redefine joint employer status, the board has determined that an employer (whether franchisee or franchisor) can be named a joint employer before any finding that an unfair labor practice has been committed. On January 8, 2016, the NLRB approved an administrative law judge's decision allowing evidence of McDonald's Corporation's joint liability with its franchisees, prior to deciding whether any labor law violations had occurred.

Continued on page 4

A No-Win Situation: The Supreme Court Declines To Resolve CAFA Circuit Split

Luke Cantrell, 901.577.8188, lcantrell@bakerdonelson.com

The Class Action Fairness Act of 2005 (CAFA) represented a major overhaul of class action lawsuits and made the federal courts available for cases not involving a question of federal law. Among the effects, CAFA greatly increased federal courts' discretion to exercise diversity jurisdiction over class action suits. This was accomplished by relaxing how the amount in controversy is determined and through major changes to the geographic diversity requirements.

Continued on page 5

Sara Turner
Executive Editor
205.250.8316

Joel Buckberg
Editor Emeritus
615.726.5639

Greetings From Hospitalitas

Hospitalitas is the Baker Donelson newsletter for our clients and friends in the hospitality industry – hotels, restaurants and their suppliers. It is published several times a year when we believe we can deliver first-class, useful information for your business. Please send us your feedback and ideas for topics you would like to know more about. True to our Southern heritage of hospitality, we'll work hard to make each visit with us something special and worth repeating.

Franchisor Protected from Unfair Competition, Not All Competition, *continued*

Rib City Franchising, LLC franchises barbeque restaurants across the United States. Rib City entered into a License Agreement with Toni Jorgenson and Way Out West Restaurant Group (WOW) to operate a Rib City franchise in American Fork, Utah. The franchisee failed to make payments required under the License Agreement and, on July 13, 2015, Rib City terminated the License Agreement.

Rib City filed a lawsuit in federal court in Utah claiming that on or around the termination date, Ms. Jorgenson transferred the Rib City Grill franchise – including client and supplier lists, menus, recipes, décor, social media account and the Rib City telephone number – to Sarah Bowen. Ms. Bowen had worked for a time as an assistant manager at the Rib City location. Ms. Bowen and her company, Culinary Designs, LLC, began operating a barbeque restaurant in the same location under the name "Pig City BBQ."

In its lawsuit, Rib City also claimed that Ms. Bowen began to promote Pig City BBQ using various social media sites such as YELP and Trip Advisor which were previously maintained to promote the Rib City Grill. According to Rib City, rather than create new profiles, Ms. Bowen simply renamed these existing web pages, resulting in Rib City's reviews, photos, and registered marks appearing under Pig City BBQ's name.

A hearing was held shortly after suit was filed and the court ordered the defendants to take any action reasonably necessary to remove the Facebook, Twitter, YELP, Trip Advisor, Four Square and YouTube website pages that were using or referencing Rib City marks. The court also required the defendants to take any action reasonably necessary to disconnect the Rib City telephone number and to take any action reasonably necessary to prevent that number from connecting to Pig City BBQ.

By this order, the court took the necessary step to protect the integrity of Rib City's registered trademark and to prevent the wrongful use of these marks in connection with a competing business. However, Rib City was not satisfied. Rib City sought a further order from the court requiring the defendant to cease all use of what it described as the confusingly similar "Pig City BBQ" name; to remove all trade dress associated with the former Rib City Grill Restaurant; to cease any and all use of Rib City's confidential, proprietary and trade secret information, "including but not limited to Rib City Grill trade secret recipes and ketchup;" and to cease operating the competing and infringing Pig City BBQ Restaurant altogether.

After further consideration of Rib City's additional requests, the court concluded that while it was proper to take action to stop the wrongful use of Rib City's registered trademark, Rib City was not entitled to the additional relief that would effectively put its new competitor out of business.

Rib City argued that its name and "Pig City BBQ" were confusingly similar, but the court disagreed. The court pointed out that the actual graphics of the respective service marks were quite different. The court found no credible evidence demonstrating that the use of the competing mark created confusion in the marketplace.

Continued on page 3

Franchisor Protected from Unfair Competition, Not All Competition,

continued

Rib City next argued that the defendant's use of its trade dress and décor was improper. In order to prevail on this claim, Rib City was required to prove that its claimed trade dress is either inherently distinctive or has acquired a secondary meaning expressly associated with Rib City in the marketplace, and that the operation of the Pig City BBQ Restaurant created a likelihood of customer confusion. The court found nothing particularly distinctive about Rib City's décor and denied the request.

Rib City also argued that Pig City BBQ had essentially copied its menu and was improperly using Rib City recipes. The court ruled that the Rib City menu is not a trade secret. It is available online. There is nothing distinctive about the menu; it contained most of the items found at any barbeque restaurant. Finally, the court noted that Rib City produced no evidence to indicate that Pig City BBQ was using its recipes, or that those recipes qualified as "trade secrets." The decision doesn't say whether Rib City had any agreements with the landlord or the managers of the franchised restaurant about continuity of the business, or protecting the system information and branding after the franchise left the chain.

In short, Rib City terminated its franchise location in American Fork, Utah. A new entity, not the terminated franchisee, began to operate a competing barbeque restaurant at that facility post-termination. The new operator initially took over Rib City's social media sites and, in doing so, used Rib City registered trademarks to promote its new barbeque restaurant. It also used a telephone number that belonged to Rib City. These actions were unlawful and properly enjoined by the court. Not satisfied, Rib City pressed for additional relief which essentially would have put Pig City BBQ out of business. In the era of fear for joint employer status that may prevent franchisors from asking for manager non-competition agreements, this case highlights the risk of not engaging in that protective practice. This opinion also reminds us that the purpose behind trademark and unfair competition laws are to prohibit and punish the wrongful use of trade names, service marks or, in certain circumstances, trade dress which consumers specifically associate with the owner of those marks. The purpose is to prevent unfair competition. The protection provided by these laws does not extend so far as to eliminate lawful competitors. The case reminds us of the old adage, "pigs get fat, hogs get slaughtered."

NLRB: Joint Liability Inquiry Can Precede Finding on Merits of Underlying Unfair Labor Practice Charge, *continued*

The Board ruled 2-1 that the administrative law judge did not abuse her discretion because she "structured the litigation in a manner that she determined would be most efficient and effective for allowing the general counsel and the charging parties to present their cases and for respondents to mount their defenses." The implication of the NLRB's decision is that a franchisor can be included in unfair labor practice proceedings even if the adjudicator has not made any finding on the merits of the underlying unfair labor charges. In this case, where the NLRB has consolidated numerous charges,

Continued on page 4

NLRB: Joint Liability Inquiry Can Precede Finding on Merits of Underlying Unfair Labor Practice Charge, *continued*

the allegations comprise 181 violations of the National Labor Relations Act (NLRA) in 30 different restaurant locations. Notably, the charges span six NLRB regions. As a result, the franchisor will be dragged into discovery, which will be expensive and time consuming. That discovery will center around whether a joint employer relationship exists, putting the joint employer issue at the forefront – well before the merits of the charge are reached.

Board member Phil Miscimarra dissented from the NLRB's decision, noting that the proceedings appear to be intended to align with the NLRB general counsel's recent "overarching" joint employment doctrines. Mr. Miscimarra also noted his prior dissent from the NLRB's decision consolidating the numerous unfair labor charges. Believing the parties and claims too numerous and dissimilar to be thrown into a single case, Mr. Miscimarra opined that the structure of this litigation will impose oppressive costs, burdens and delays on the parties, the NLRB, and reviewing courts. To this point, McDonald's estimates that it has already spent more than $1 million on the NLRB litigation, while it will owe no more than $50,000 if it is found to be jointly liable for the unfair labor practices committed at the franchisee establishments.

As this has played out, it has become clear that the NLRB decision has opened the door for wide-ranging discovery on the issue of joint employment status before any determination of the merits of an unfair labor practice has been made. For instance, on January 21, 2016, Chicago-area federal judge Samuel Der-Yeghiayan ordered nine franchisees to comply with NLRB subpoenas requesting documents and records the NLRB said would allow it to determine how the fast food corporation has partnered with its franchisees and has organized its business. Judge Der-Yeghiayan determined that "[g]iven the broad range of relevant factors for a joint employer determination, the NLRB necessarily needs to seek a broad range of information in order to properly address its joint employer allegations." Remarkably, McDonald's claims that it has produced more than 160,000 documents in response to NLRB requests. With the NLRB's January 8 decision, this type of discovery will become more common.

The NLRB's recent decision comes in the wake of its ruling last year that McDonald's headquarters in Oak Brook, Illinois, and local franchises can be held jointly responsible for violating federal labor laws. There, the NLRB determined that McDonald's engaged in sufficient control over its franchisees' operations, beyond protection of the brand, to make it a putative joint employer with its franchisees, sharing liability for violations of labor laws the agency enforces. This is despite McDonald's contention that its franchisees – which own 90 percent of the company's more than 14,000 U.S. restaurants – set wages and control working conditions independently within their restaurants.

The alleged unfair labor practices include spying, unlawful promises of increased benefits, discrimination against pro-union workers, threats of termination, threats of closing McDonald's restaurants, unlawful reductions in work hours, and intimidation tactics including failing to post work schedules and pretending to choke an employee to dissuade union representation.

Continued on page 5

NLRB: Joint Liability Inquiry Can Precede Finding on Merits of Underlying Unfair Labor Practice Charge, *continued*

Previously, the NLRB had determined that a franchisor could be considered a joint employer only if it directly employed or controlled the franchisee's workers. Under the NLRB's new interpretation of joint employment, a franchisor can be jointly liable for unfair labor practices committed by a franchisee if the franchisor wields indirect or potential control over the franchisee's workers. Under the new standard, it will be much easier for franchisors to be named joint employers under the NLRA. Not only would this make such employers potentially jointly liable for unfair labor practices, but it would also impact their obligations to engage in collective bargaining.

In a report prepared by for the International Franchise Association, IHS Global Insight recently estimated that approximately 781,794 franchise establishments exist in the United States. The IFA also estimates that the franchise industry provides jobs for more than 8 million workers. The NLRB's continued efforts to enlarge joint liability for franchise relationships may well affect the growth of the franchise economy.

A No Win Situation: The Supreme Court Declines To Resolve CAFA Circuit Split, *continued*

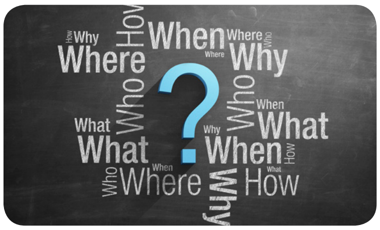
Prior to CAFA's enactment, at least one class member was required to assert a claim of at least $75,000 for a federal court to exercise diversity jurisdiction over a case. While that requirement did not always prove problematic, many of today's class actions involve automobile recalls, cell phone fees, and convenience charges that do not come close to $75,000 on an individual level. Class members and defendants in those cases could not proceed in federal court based on diversity jurisdiction alone. CAFA increased the amount in controversy requirement to $5 million, but the requirement can now be met by combining all the class members' claims to reach the threshold.

CAFA also changed the requirement that all plaintiffs be geographically diverse, or citizens of different states, from all defendants to allow federal diversity jurisdiction to be exercised. If one plaintiff is diverse from one defendant, geographic diversity is met under CAFA.

The Supreme Court has not been shy about weighing in on CAFA jurisdiction issues in the past, such as whether a removing defendant must include evidence supporting the basis for removal or if a statement alleging grounds for removal is enough, so many assumed that the Court would address the latest issue head-on.

Continued on page 6

NLRB: Joint Liability Inquiry Can Precede Finding on Merits of Underlying Unfair Labor Practice Charge, *continued*



An Unanswered Question Results In A Circuit Split

Due to the relaxation of the requirements for diversity jurisdiction, many more class actions have made their way into federal court, either through filing there or by removal by defendants seeking an alternative forum to state court. One resulting anomaly is when a case is removed to federal court and the court later finds it does not have jurisdiction to hear the case, and the state court is also without jurisdiction for the same reason. The question then exists, as was presented to the Supreme Court in *Layne Energy Inc. et al v. Catron*, of whether the federal court may dismiss the case or must remand the case even if the state court does not have jurisdiction and will have to dismiss it at the state court level.

After the class action was removed to federal court in Layne, the sole named class representative admitted that he could not have been injured by the conduct alleged in the case and, therefore, did not have standing to be a member of the class. If the case was remanded, the state court would not have jurisdiction over the named plaintiff either, so the case would be dismissed by the state court and the remand is futile.

A circuit split has resulted over this issue. The two approaches of the different circuits are as follows:

The First, Fifth, and Ninth Circuits have found, and the Second Circuit has indicated that it would follow suit, that the federal district court judge is entitled to dismiss the case instead of remanding to state court when remand would be futile. The primary reason for what is termed the "futility exception" is to avoid a waste of judicial resources.

The Third, Fourth, Sixth, Seventh, Tenth and Eleventh Circuits have held directly opposite and rejected this "exception" based on the language of 28 U.S.C. § 1447(c). Section 1447(c) states in relevant part that "[i]f at any time before final judgment it appears that the district court lacks subject matter jurisdiction, the case shall be remanded." Although those six circuits have affirmed dismissals in cases where remand would be futile, those same circuits have held that they are prevented from recognizing the "exception" because the language of § 1447(c) mandates that "the case shall be remanded."

The Supreme Court's Decision Fails To Mend The Divide

In *Layne*, the petitioners recognized "a classic circuit split that the Supreme Court should settle." The petitioners asked the Court to reverse the Tenth Circuit's decision that once again affirmed that a district judge in that circuit must remand, and not dismiss, a suit even when the parties and the court agree that the sole named plaintiff lacks standing to bring the suit whether in state or federal court.

Continued on page 7

NLRB: Joint Liability Inquiry Can Precede Finding on Merits of Underlying Unfair Labor Practice Charge, *continued*

As the petitioners stated in their Petition for Writ of Certiorari to the Supreme Court, "Had this case been brought in the First, Fifth, or Ninth Circuits, this action would have been dismissed rather than remanded, and Defendants would not be forced to relitigate in state court a dispositive finding, which they already obtained from the district court, that Plaintiff had no standing or right to bring this lawsuit." Despite the opportunity to resolve this circuit split, the Supreme Court denied certiorari and chose not to do so, declining the opportunity to acknowledge a futility exception to § 1447(c) and perpetuating this circumstance where a case ends up in a no-win purgatory and wastes judicial resources, without the potential of a different outcome.

Lessons Learned from Recent FTC Enforcement Cases Against LabMD and Wyndham

Samuel L. Felker, 615.726.5558, samfelker@bakerdonelson.com
Gina Ginn Greenwood, 478.765.1804, ggreenwood@bakerdonelson.com
Eric Setterlund, CIPP/US, 423.209.4221, esetterlund@bakerdonelson.com

On the shifting sands of cyber security regulation, it is important to understand the outcome of two recent enforcement cases brought by the Federal Trade Commission (FTC) – one against clinical lab services company LabMD, Inc. and the other against international hotel giant Wyndham. In the former case, LabMD was accused of security breaches that allegedly exposed its patients' private information, but on November 19, 2015, an administrative law judge dismissed the FTC's case against LabMD on the merits, finding the FTC failed to carry its burden of proof under Section 5 of the Federal Trade Commission Act (FTC Act) that LabMD's security failures caused, or were likely to cause, substantial injury to consumers. Although the FTC has appealed, this represents a successful and serious challenge to the FTC's authority to regulate cyber security breaches, particularly in cases where there is no demonstrated "injury" from the data breach.

On the other hand, the long and contentious case against Wyndham Hotels and Resorts, LLC (Wyndham) and certain of its affiliates ended in settlement with the FTC after the Third Circuit upheld the FTC's statutory authority to regulate and enforce cyber security breaches. The Wyndham settlement, announced December 9, 2015, provides insight into what the FTC considers reasonable data security, particularly when subsidiaries and franchisees are involved.

We will discuss both cases and then provide important "takeaways" for companies to consider in developing their cyber security procedures.

Continued on page 8

Lessons Learned from Recent FTC Enforcement Cases Against LabMD and Wyndham, *continued*

Dismissal of the FTC's Case Against LabMD

In the August 28, 2013, complaint, the FTC charged that because of two security incidents, LabMD, a clinical testing laboratory, failed to provide reasonable and appropriate security measures for personal information and this conduct caused or was likely to cause substantial injury to consumers. The FTC alleged that LabMD was liable for "unfair" acts or practices under Section 5 of the FTC Act, thereby exposing personal information of up to 10,000 customers to hackers in two separate incidents in 2009 and 2012.

Section 5 of the FTC Act (15 U.S.C. § 45(n)) states that the FTC "shall have no authority to declare unlawful an act or practice on the grounds that such act or practice is unfair unless [1] the act or practice causes or is likely to cause substantial injury to consumers, [2] which is not reasonably avoidable by consumers themselves and [3] not outweighed by countervailing benefits to consumers or to competition."

However, the administrative law judge found that the FTC failed to establish an unfair trade practice because the FTC failed to prove the first prong of the three-part test above – that the alleged unreasonable conduct caused or was likely to cause substantial injury to consumers. Specifically, the evidence failed to prove that the limited exposure of the data resulted, or was likely to result, in any identity theft-related harm. The evidence also failed to prove that embarrassment or similar emotional harm likely to be suffered from the exposure is a "substantial injury" where there is no proof of other tangible injury. Lastly, the theory that the company's data is "at risk" of a future data breach was also rejected. In rendering the decision, the administrative law judge stated,

> "To impose liability for unfair conduct under Section 5(a) of the FTC Act, where there is no proof of actual injury to any consumer, based only on an unspecified and theoretical "risk" of a future data breach and identity theft injury, would require unacceptable speculation and would vitiate the statutory requirement of "likely" substantial consumer injury. At best, [the FTC] has proven the "possibility" of harm, but not any "probability" or likelihood of harm. Fundamental fairness dictates that demonstrating actual or likely substantial consumer injury under Section 5(n) requires proof of more than the hypothetical or theoretical harm that has been submitted by the government in this case."

Accordingly, the complaint was dismissed. The FTC promptly appealed the decision to the commissioners of the FTC without specifying any new grounds. Click here to see the pleadings in the LabMD – FTC case.

The Wyndham Settlement

Several years ago, Wyndham was the victim of sophisticated cyberattacks by criminal hackers, who accessed customer information at certain Wyndham Hotels and Resorts-brand hotel properties. Wyndham promptly alerted law enforcement agencies, retained computer forensic experts, implemented significant security enhancements and assisted franchised Wyndham Hotels and Resorts-brand hotels

Continued on page 9

Lessons Learned from Recent FTC Enforcement Cases Against LabMD and Wyndham, *continued*

in reinforcing their information security. Wyndham also made prompt efforts to notify the hotel customers whose information may have been compromised, and offered them credit monitoring services.

After an investigation, the FTC filed a complaint alleging violations of Section 5 of the FTC Act, 15 U.S.C. § 45, which bars "unfair or deceptive acts or practices in or affecting commerce." The FTC essentially argued that hackers had gained access to the network of a Wyndham franchisee and then exploited security on the hotel chain's corporate network to steal credit card information from customers of other Wyndham franchisees.

In the past decade, the FTC had brought more than 40 such enforcement actions against companies alleging data security violations. In each of those actions, the defendant entered into a settlement agreement (consent decree) with the FTC rather than litigating the claims. However, Wyndham took a novel and aggressive approach, defending on the basis that the FTC had no authority to "impose general data-security standards" upon businesses in all industries in the absence of specific legislation. Earlier this year, the Third Circuit decided otherwise and confirmed the FTC's statutory authority to regulate cyber security practices under the unfairness prong of Section 5 of the FTC Act by bringing lawsuits against companies over data security practices the FTC deems unreasonable.

Following are the key terms of the settlement between Wyndham and the FTC:

- Wyndham will not pay any monetary relief.
- The company is granted a Safe Harbor if it continues to meet certain requirements for "reasonable information security" outlined in the FTC's consent order.
- The consent order applies only to payment card information, and does not apply to any other categories of personally identifiable information. Payment Card Industry (PCI) certification will satisfy Wyndham's reporting requirement and provide the basis for the Safe Harbor.
- The duration of Wyndham's obligations under the consent order will in no event be longer than 20 years, and in several areas will be shorter.

Wyndham issued the following statement:

> "We are pleased to reach this settlement with the FTC, which does not hold Wyndham liable for any violations, nor require Wyndham to pay any monetary relief. We chose to defend against this litigation based on our strong belief that we have had reasonable data security in place, and that the FTC's position could have had a negative impact on the franchise business model. This settlement resolves these issues, and sets a standard for what the government considers reasonable data security of payment card information. Safeguarding personal information remains a top priority for our company at a time when companies and government agencies are increasingly the targets of cyberattacks."

Click here to see the pleadings in the Wyndham – FTC case.

Continued on page 10

Lessons Learned from Recent FTC Enforcement Cases Against LabMD and Wyndham, *continued*

Key Takeaways

Would-be breach defendants and data owners and processors everywhere should consider the following takeaways.

(1) For now, it will be substantially more difficult for the FTC to act arbitrarily in cases in which no actual harm can be shown. The enforcement requirements set forth by the administrative law judge in the LabMD case parallel the same type of pleading and proof of injury standards that private litigants have had to meet in connection with the majority of data breach cases that have been decided. In order to be liable under Section 5 of the FTC Act for failing to maintain "reasonable and appropriate" security for personal information, the data breach must have "caused or be likely to cause" actual and substantial consumer injury – which has now been interpreted to mean that emotional harm or an increased risk that hypothetical or theoretical harm is not enough. The standard to which FTC was held is much like the "actual injury" constitutional standing requirements that have plagued plaintiffs in civil breach litigation cases.

(2) Defendants currently in the FTC's crosshairs may find themselves with better settlement bargaining power. The FTC has secured numerous settlements and consent decrees (53 of 55 data security cases) by asserting that the company's failure to protect personal information, alone, was sufficient to establish the "substantial injury" required by Section 5. Following the LabMD ruling, at least for now, companies will be in a much stronger bargaining position where there is no actual injury to customers or others as a result of a data breach. In the past, the FTC acted as though it had total latitude to bring actions in the absence of likely harm, but this decision changes that dynamic as more enforcement targets may challenge the FTC's authority. Further, the Wyndham settlement's focus solely on credit card data, and not globally on other forms of personally identifiable information, indicates that Wyndham had the upper hand in negotiations in several respects.

(3) The FTC's authority to bring enforcement actions against alleged "violators" may not reach as far as the Office for Civil Rights (OCR) authority over health care companies and their business associates. When a complaint or breach of unsecured protected health information is investigated by OCR, the case is assessed based on strict compliance with the applicable HIPAA Privacy, Security and/or Breach Notification Rules. OCR need not prove actual, or potential, harm to attempt to levy large penalties. In contrast, should the administrative law judge's decision in the LabMD case stand, the FTC will now have to demonstrate actual or probable harm to consumers – perhaps significantly limiting the FTC's enforcement capabilities. If the FTC is not successful in overturning the LabMD decision, the FTC could potentially attempt to implement its own regulations in an effort to permit easier enforcement.

(4) The FTC for the first time provided valuable guidance about what it views as reasonable cyber security procedures to protect credit card information, particularly where there are franchisees and affiliates involved. Rather than addressing Wyndham's comprehensive data security program, the Consent Order specifically notes safeguards that should be utilized to protect against theft of payment

Continued on page 11

Lessons Learned from Recent FTC Enforcement Cases Against LabMD and Wyndham, *continued*

card information. The settlement incorporates the PCI DSS as the applicable standard to be applied in the ongoing audits of Wyndham. By adopting this payment card industry standard, the FTC provided valuable insight into the procedures that it deems reasonable related to credit card data. The settlement also mandated certain firewall procedures between the company's servers and its franchisees, also required by PCI DSS, which is instructive as to what the FTC expects of any company dealing with third parties.

Looking Ahead

As mentioned, the FTC has already appealed the administrative law judge's ruling in the LabMD case, and in addition, numerous lawsuits have been filed related to the case. There is parallel litigation ongoing between LabMD and cyber security firm Tiversa Holding Corp., with the latter accused of stealing LabMD's confidential customer records and leaking them to the FTC when LabMD did not hire Tiversa to remediate the alleged breach. Tiversa in turn has sued LabMD and its CEO for defamation for accusing the company of hacking and the alleged extortion scheme. In yet another proceeding, LabMD has sued the agency lawyers for costs, saying it was ruined by an illegal and unethical prosecution.

Now that the FTC's case against Wyndham is resolved, it is important to observe the FTC's enforcement activities regarding theft of credit card information to see if the guidelines provided in the settlement will be applied in other cases. For example, only one week after the Wyndham settlement, the FTC announced a $100 million settlement with LifeLock, Inc. resolving allegations that LifeLock's advertising and data security practices violated a 2010 court order prohibiting it from misrepresenting its identity theft protection services and requiring it to establish and maintain a comprehensive information security program. In its press release, the FTC commented that PCI DSS certification is insufficient in and of itself to establish the existence of reasonable security protections, noting that the Wyndham order calls for a number of additional significant protections, including the implementation of risk assessments, certification of untrusted networks and certification of the assessor's independence and freedom from conflicts of interest. In its press release, the FTC cautioned, "As we have long emphasized, the reasonableness of security will depend on the facts and circumstances of each case."

Baker Donelson's privacy and security team will continue to monitor what is expected to be a lengthy appeal process for LabMD and report on other notable legal developments. Despite the recent FTC setback in LabMD, we still believe that once a company becomes an FTC target, it is unlikely to give up without a fight. Therefore, it is important for businesses with consumer data (including patient data and credit card information) to work with attorneys and IT consultants to implement reasonable and appropriate privacy and security measures to reflect lessons learned from the FTC's regulatory activities, and to prepare for future breaches.

For more information about how this ruling may affect your business or for assistance with your litigation, compliance or breach preparedness and response needs, contact the authors of this article or any member of the Firm's Privacy and Information Security Team.

Quick Takes

Look for Us in San Antonio!
Look for Baker Donelson at IFA Conference booth # 520 in San Antonio February 21–23. We'll be offering up a famous Nashville treat, as well as information about the Franchisor Toolkit, including the new mobile app.

Baker Donelson Adds 20 Attorneys and Staff from Busch White Norton; Expands Presence in Atlanta and Florida
In January Baker Donelson announced the addition of nine attorneys to its Financial Services and Real Estate Groups. The attorneys, all of whom were previously with the firm of Busch White Norton, will expand Baker Donelson's presence in both Georgia and Florida. Four attorneys joined Baker Donelson's Atlanta office and five joined in Florida, bringing a total of 11 paralegals and other staff.

"This is a tremendously talented group of professionals who have extensive experience and solid reputations," said Ben C. Adams, chairman and chief executive officer of Baker Donelson. "Their addition to the Firm gives us the opportunity to add to the depth of two core practice areas while strengthening our foothold in Florida and growing our presence in Atlanta."

These attorneys include Bryan E. Busch, Mahira Khan, Christopher Y. Mills, Laura H. Mirmelli, Matthew B. Norton, Kyle Peters, Brian D. Pierce Chantal Pillay and Debbie Satyal.

Amy Elder Elected to Board of Trustees of the International Association of Gaming Advisors

Amy Kebert Elder of Baker Donelson has been elected to a second consecutive three-year term on the Board of Trustees of the International Association of Gaming Advisors (IAGA). Ms. Elder, of counsel in the Firm's Jackson office, focuses her practice on gaming regulatory and business law in Mississippi and Louisiana. She represents all types of domestic and international gaming-related clients and assists them in addressing a broad range of regulatory issues and transactional matters, assisting with development, licensing, financing, transfers of ownership, training and compliance, internal investigations and more. Ms. Elder is a graduate of the University of Mississippi School of Law and is a member of the Mississippi Bar, the American Bar Association and the Mississippi Women Lawyers Association.

As a member of the IAGA's Board of Trustees, Ms. Elder is responsible for developing and implementing all measures which promote the objectives of the organization. The IAGA is an association of attorneys, financial experts, casino executives and regulators in the gaming industry. IAGA's purpose is to provide leadership in addressing issues affecting the industry. Formed in 1980, it has grown to more than 300 members worldwide.

Continued on page 13

Quick Takes, *continued*

Joel R. Buckberg Named Leader of Firm's Commercial Transactions and Business Counseling Group

Joel Buckberg has been named the first practice group leader of Baker Donelson's newly formed Commercial Transactions and Business Counseling Practice Group.

"This group was formed to meet the needs of business clients and potential business clients for legal services in specialty practice areas, and to assist with counseling on their commercial activity. Our practice group serves clients in planning and pursuing their business interests in global trade and international business, gaming, hospitality, franchising, travel industry, aviation and medical office facility ownership and management, as well as serving as general counsel to businesses without in-house lawyers. I look forward to working with these highly regarded practitioners as they continue to successfully serve our clients," said Mr. Buckberg, who leads more than 90 attorneys across the Firm's 20 offices.

Mr. Buckberg is a shareholder in the Firm's Nashville office, where he counsels clients on business transactions and operations, particularly in hospitality, franchising and distribution, including strategic planning, development, disclosure, equity and debt financing, mergers and acquisitions, system policy and practice development, regulatory compliance and commercial contracts. Prior to joining Baker Donelson, he was executive vice president and deputy general counsel of Cendant Corporation.

Matthew McLaughlin Named to Faculty of University of Vermont Craft Beer Program

Matthew P. McLaughlin of Baker Donelson has been selected to serve on the faculty for the University of Vermont Business of Craft Beer Professional Certificate Program. One of only a handful of schools in the country to offer this type of program, the University of Vermont will launch the program in the spring 2016 semester. Mr. McLaughlin will be involved in the "Fundamentals of Craft Beer" course, which will focus on craft beer trends, styles, branding, merchandizing, marketing, finance, beer regulations and distribution.

Mr. McLaughlin, who chairs Baker Donelson's craft brewery and craft distillery industry focus team, has extensive expertise working with regional craft breweries and craft distilleries in all aspects of their operations. He advises industry participants on business entity formation, ownership structure, startup financing and expansion financing, and files and registers trademarks and protects all forms of intellectual property. Mr. McLaughlin oversees the land use approval process for the construction and operation of craft breweries and craft distilleries, and drafts and reviews distribution agreements, licensing agreements, and employment-related agreements. He advises clients on Alcohol and Beverage Control (ABC) and Alcohol and Tobacco Tax and Trade Bureau (TTB) license applications and the filing of other necessary federal and state permits. He regularly consults craft breweries, craft distilleries, and brewpubs on alcohol and beverage laws, and he advises craft breweries, brewpubs and others in the industry on economic development incentives, and legislative and policy matters that impact the alcohol industry.

Upcoming Franchise Business Network Dates

Baker Donelson is pleased to serve as local host for the International Franchise Association's quarterly Franchise Business Network events in Alabama; Tennessee; Louisiana; and Orlando, Florida. Future meeting dates are Tuesday, April 12; Wednesday, July 20; and Wednesday, October 19. If you'd like to be added to our mailing lists for this event, please email Laura Ellis.