American Bar Association
43rd Annual Forum on Franchising

W-20 AGE OF DISRUPTION: CURRENT ISSUES FOR RESTAURANT FRANCHISES

Anne P. Caiola
Caiola & Rose, LLC
Atlanta, Georgia

Brittany Johnson
Starbucks Coffee Company
Seattle, Washington

and

Andra Terrell
Global Cajun Operating Company
Atlanta, Georgia

October 27-30, 2020

©2020 American Bar Association

TABLE OF CONTENTS

I. INTRODUCTION 1

II. DIGITAL ORDER & DELIVERY 1

A. Rise of the Digital Order & Delivery Channel 1

B. Understanding Aggregator Models 2

1. Marketplace 2

2. End-to-End 3

C. Implementing Third-Party Delivery Services in a Franchise System 3

3. Determine Approach to Launch 4

4. Anticipating Commonly Negotiated Issues 6

5. Updating Franchise Agreements and Disclosure Documents 10

D. Mounting Tension 11

1. Disintermediation 11

2. Competition from Aggregators 12

3. Prepare for Platform Access Issues 13

4. Consolidation 14

5. Legal Developments 14

6. Emerging Technologies 15

III. DATA PRIVACY AND PROTECTION 15

A. Understanding the Landscape 15

1. Technology has caused more data to be collected 15

2. Uses and Benefits of Data in Franchise Systems 16

B. Legislative and Regulatory Disruptions 27

1. European Union General Data Protection Regulation (the “GDPR”) as an initial privacy disrupter 29

2. California Consumer Privacy Act (the “CCPA”) adding onto the issue 34

3. Other State Privacy Laws Giving Opt-Out Rights 38

4. Additional state legislation/regulations to come 39

C. Data Collection and Ownership.....41

D. Data Breach Responses 42

E. Changes to the Franchise Agreement.....46

IV. FOODBORNE ILLNESS IN A FRANCHISE SYSTEM.....47

A. Legal Exposure within a Franchise System.....47

1. Franchisor and Franchisee liability to consumers 47

2. Franchisor liability to franchisees.....50

3. Liability of officers and directors of franchise systems 50

4. Suppliers' liability to a franchise system.....51

B. Navigating a Minefield – Responding to a Public Health Threat 52

1. Notice to consumers.....52

2. Notifying insurance carriers 53

3. Impact of Communications on Attorney Client Privilege.....54

C. The Foodborne Illness Litigation Landscape 56

1. Exposure to class action lawsuits by consumers 56

2. Indemnification duties of suppliers and recovery of economic losses 57

3. Insurance coverage requirements and coverage disputes.....57

D. Preparing for an Outbreak.....58

1. Robust supply chain agreements.....58

2. Internal preparedness.....58

V. OTHER DISRUPTORS AFFECTING RESTAURANT FRANCHISE SYSTEMS.....59

A. Global pandemics, global warming, and natural disasters.....59

B. ADA Compliance in emerging technologies 60

C. Emerging Trends in Employee Pay and Benefits 61

1. Advanced Payment Products 61

2. Pandemic-triggered changes in state medical leave laws 62

VI. CONCLUSION 63

AGE OF DISRUPTION: CURRENT ISSUES FOR RESTAURANT FRANCHISES

I. INTRODUCTION

Facing disruption is now, more than ever, a part of conducting business in today's world. For franchise businesses, the question is no longer *whether* the business will face disruption. Instead, the questions now focus on *what* form the disruption will take, *when* it will emerge, and *how* to adapt.

Restaurant franchises, in particular, have encountered many significant disruptors in recent years. Some disruptors are unique to food businesses, while others apply to businesses operating across various industries. What remains common among these disruptors is that each has the potential to pose significant risk to a restaurant franchise's business model, reputation, and even its long-term viability. And each disruptor, at a minimum, could force significant change within the business.

This paper explores recent disruptors in the restaurant industry, including the use of third-party digital delivery services, protecting against and responding to cyber breaches, ensuring that digital resources comply with recent developments in the law, addressing illness outbreaks (whether foodborne or otherwise), responding to changes in workforce and pay trends, and even preparing for and recovering from natural disasters. The paper also outlines best practices for mitigating these risks to help businesses stay current and competitive.

II. DIGITAL ORDER & DELIVERY

The meteoric rise of third-party digital delivery services forever changed the restaurant industry. Third-party digital delivery service providers, referred to in this article broadly as "aggregators," made online ordering and delivery an accessible option for businesses ranging from small, independent restaurants to large, multi-national brands. As a result, many customers now expect restaurants to offer a seamless digital ordering and delivery experience, regardless of size or location. In an effort to capitalize on this newly-accessible channel and to meet changing customer demands, restaurants joined forces with aggregators at an increasingly rapid pace. As a result, aggregators earned their seat at the metaphoric dinner table, causing deep and wide-ranging disruption in the restaurant industry.

A. <u>Rise of the Digital Order & Delivery Channel</u>

The delivery channel itself is not new. For decades, restaurants have offered delivery directly to customers. Consumers are very familiar with the direct model. In the direct model, a customer places an order directly with the restaurant, usually by phone, and the restaurant's own driver transports the food to the customer's designated location. [1] Even as recently as 2016, the vast majority of delivery orders placed by customers used the direct model.[2] Some brands, such as Domino's, have also seen success converting the direct model to a proprietary electronic platform, complete with mobile ordering and tracking capabilities.

---

[1] Carol Hirschberg et al., *The Changing Market for Food Delivery*, McKinsey & Co. (Nov. 9, 2016), https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/the-changing-market-for-food-delivery.

[2] *See id.*

What is new is the emergence of digital technology within the delivery channel. Aggregators like Uber Eats, Grubhub, Just Eat, Delivery Hero, and many others, created online digital platforms and applications that made it more convenient than ever for customers to purchase food for delivery without ever picking up the phone or even interacting directly with the purveyor. As convenience, use, and demand for digital delivery increased, so has the growth of the entire delivery channel. Indeed, some predict that the digital delivery channel will continue to grow by as much as fourteen percent per year and may become a $200 billion industry by 2025.[3] The growth is likely to continue through the end of the decade, with some predicting the digital delivery industry could grow to a $385 billion industry by 2030.[4] Following the COVID-19 pandemic, the digital delivery channel could grow even more quickly as even broader swaths of the consumer base select digital delivery technology as an alternative to in-person dining.[5]

B. Understanding Aggregator Models

All aggregators utilize a proprietary digital platform accessed by customers. On the platform, a customer can view multiple restaurants, read menus, place an order, and schedule delivery. Some platforms allow other functionality, such as allowing customers to share restaurant reviews or real-time delivery tracking features.

While all aggregators use a digital platform, not all aggregators are created alike. Two primary aggregator models exist: the marketplace model and the end-to-end model.[6] Each model offers different services, provides different customer experiences, and includes different payment structures. Understanding the aggregator business model is important for any franchise restaurant business considering launch of digital delivery because the specific business model involved will directly impact how the brand shows up to customers, the fees charged by the aggregator, and the legal and brand risks encountered by the restaurant and franchisor.

1. Marketplace

Marketplace aggregators provide a digital platform that customers can use to browse multiple restaurants, compare menus and prices, place orders, and make payment. However, marketplace aggregators do not themselves provide delivery services.[7] Customers either pick up their order at the restaurant, delivery is provided by the restaurant itself, or delivery services are provided by a different third-party logistics service.

Marketplace aggregators appear to be losing favor. While many aggregators began as marketplace aggregators, over time, their technologies evolved, and their logistics capabilities increased. Similarly, over time, customer behavior shifted in some cases to a preference for full-service platforms able to provide a single source of contact for the entirety of a delivery transaction. These changes slowly caused many aggregators, like Grubhub, Foodpanda, Delivery

---

[3] *See id.*

[4] Michael Houck, *The Future of Food (Delivery)*, MEDIUM (Jul. 21, 2019), https://medium.com/@houck/the-future-of-food-delivery-report-d4df49789632 (citing a study of the accessible market for food delivery).

[5] Sabine Becker et al., *Delivering When It Matters*, MCKINSEY & CO. (Apr. 14, 2020), https://www.mckinsey.com/industries/retail/our-insights/delivering-when-it-matters-quick-service-restaurants-in-coronavirus-times.

[6] *See* Hirschberg, *supra* note 1.

[7] *See id.*

Hero, and Just Eat, to offer in-app delivery services, shifting them to end-to-end aggregators (discussed below), in some or all markets. While a few of these businesses still operate under marketplace aggregator functionality in limited markets or in captive facilities like college campuses, it appears that marketplace aggregators are slowly being replaced by end-to-end aggregators.

Marketplace aggregators are usually less expensive for restaurant businesses. They generate revenue by charging a commission fee to restaurants equal to a defined percentage of each sale. Because delivery services are not provided by a marketplace aggregator, the commission is usually less than that charged by an end-to-end aggregator. Also, unlike the end-to-end aggregator model, consumers typically are not charged any additional fee by the aggregator. But, if a restaurant or logistics company provides the physical delivery of the products, that party may charge an additional fee to the consumer.[8]

2. End-to-End

End-to-end aggregators provide the most comprehensive suite of services. These aggregators not only offer the browsing, ordering, and payment services typically available through marketplace aggregators, but they also offer delivery and related logistics services. This type of aggregator allows customers to have orders delivered to their designated location and, potentially, provides real-time delivery status tracking. Usually, the end-to-end aggregator uses its own logistics platform to match a platform delivery driver to the task of picking up the food at the restaurant and delivering it to the customer.

The convenience and seamless experiences offered by end-to-end aggregators are not cheap. In fact, end-to-end aggregators are typically the most expensive option. Like marketplace aggregators, end-to-end aggregators charge restaurants a commission fee based on the total amount of the transaction.[9] The commission rate charged by end-to-end aggregators is typically higher than those charged by marketplace aggregators because of the more comprehensive services provided, primarily delivery. Commissions commonly range from fifteen percent to as much as thirty percent of each order.[10] In addition, customers pay a delivery fee directly to the end-to-end aggregator.[11] Consumers may also choose (or be encouraged to) add a tip.

C. Implementing Third-Party Delivery Services in a Franchise System

The digital restaurant delivery ecosystem is complex, and the stakes can be high. As detailed below, each party involved in this ecosystem has a different set of objectives and those objectives sometimes conflict with those of the other parties.

Consumers increasingly expect seamless and convenient digital ordering and meal delivery services. They want convenience, quality, and speed, and are willing to pay for it. But, if the total costs of the transaction after factoring in both the fees payable to the aggregator and the

---

[8] *See id.*

[9] *See id.*

[10] *See* Mike Isaac & David Yaffe-Bellany, *The Rise of the Virtual Restaurant*, N.Y. TIMES (Apr. 14, 2019), https://www.nytimes.com/2019/08/14/technology/uber-eats-ghost-kitchens.html.

[11] *See* Hirschberg, *supra* note 1.

prices charged by the restaurant are too high, the customer might balk.[12] In those situations, the consumer might choose a lower-priced restaurant, an aggregator platform with a lower delivery fee, or even opt not to order from a restaurant at all. Consumers also expect delivery to be speedy, food quality to be excellent, and the platform to offer a variety of restaurants from which to choose.

Restaurants feel the pressure to meet consumer demands, to reach new and existing customers, and to remain competitive by operating in channels where customers and competitors are. If the restaurant franchise does not have its own proprietary digital delivery platform, it may determine that it has little choice other than to partner with an aggregator. However, this comes at a potentially steep price. Restaurants already operate on notoriously thin margins. If those slim margins are further eroded by the potentially material commissions charged by an aggregator, there is risk that each digital delivery transaction becomes unprofitable. There is also an open question of whether sales made via the digital delivery channel are truly incremental or whether such sales cannibalize more profitable direct sales between the restaurant franchise and the customer.[13] Further, by inserting a third party into the customer relationship, the purveyor cedes some control over the customer relationship, customer data, and the customer experience to the aggregator.

Competition among aggregators is steep. While there are still many different aggregators operating worldwide, recent years have brought significant pressure from investors and massive consolidation among aggregators.[14] This has resulted in a few major aggregator players within each region competing against each other to attract and retain customers. There is also significant pressure among aggregators to meet customer demand for a broad assortment of food options. The pressure to provide a broad assortment of food offerings also results in aggregators competing against each other to onboard the most restaurants and also to be the exclusive platform to offer certain brands and restaurants that are particularly popular. Take all of this together with the fact that some aggregators have yet to become profitable, and it is clear that the aggregators, too, face headwinds.[15]

This ecosystem is further complicated when the restaurant business involved is a franchise system. The following sections discuss the key issues restaurant franchise businesses should consider when evaluating partnering with an aggregator.

3. Determine Approach to Launch

a. Mandatory or Voluntary Participation

Franchise restaurant businesses partnering with aggregators should consider whether participation in the platform within the franchise system is mandatory or optional. Requiring participation may be attractive for a brand because it could provide the franchisor with additional

---

[12] *See* M. Houck, *supra* note 4.

[13] *See* Zach Goldstein, *The Four Horsemen of the Restaurant Apocalypse?*, MEDIUM (Sept. 12, 2019), https://medium.thanx.com/four-horsemen-restaurant-apocalypse-64947b3d9657.

[14] Sarwant Singh, *The Soon to Be $200B Online Food Delivery Is Rapidly Changing the Global Food Industry*, FORBES, (Sept. 9, 2019), https://www.forbes.com/sites/sarwantsingh/2019/09/09/the-soon-to-be-200b-online-food-delivery-is-rapidly-changing-the-global-food-industry/#1d8830e6b1bc.

[15] Brenna Houck, *Uber Eats Is Costly to Uber*, EATER (May 1, 2019), https://www.eater.com/2019/5/1/18524180/uber-eats-ipo-sec-filing-restaurant-food-delivery-app-profits.

leverage during negotiations with an aggregator that may be seeking an exclusive relationship with the brand.

Franchisors with flexible and robust contractual language allowing them to require franchisee participation in digital delivery or other e-commerce programs are in the best position to require system-wide participation. However, given the fairly recent birth of the digital delivery channel, many franchise agreements likely lack a clear contractual basis for requiring franchisee participation.[16]

Absent clear language allowing the franchisor to require participation in digital programs like digital delivery, the franchisor may consider whether to require participation by designating participation in digital delivery as part of the "system" that, under existing agreements, the franchisor controls and has the right to update through operations manual changes or otherwise.[17] This approach may be unpopular because in addition to not being explicitly permitted by the underlying franchise agreement, the digital delivery channel fundamentally changes the franchisee's business model and, consequently, the franchisee's economic position associated with each sale. Accordingly, this approach should be considered with caution and with reasonable notice before required participation begins.

Alternatively, franchisors may consider allowing franchise locations to participate in digital delivery on a voluntary basis. This approach allows franchisees to determine for themselves whether the benefits associated with joining forces with an aggregator justify the potentially steep costs. The optional approach also may pose a minimal risk to the customer experience if the brand has another location participating in the platform within the customer's delivery area because, even if not all brand locations participate, the brand's sale will not be lost altogether.[18] A franchisor seeking to achieve system-wide participation could also consider creating a structure that incentivizes franchisees to participate. For example, a franchisor could offer reduced fees, royalties, or other relief to franchisees that voluntarily opt into the platform. The optional approach could, however, pose problems for franchisors because it could inadvertently create two tiers of franchisees, those who participate in the platform and those who do not. Creating a structure that results in two categories of franchisees can cause complexities for franchisors attempting to compare results and implement uniform standards within the system. It could also require careful consideration of Franchise Disclosure Document disclosures, including disclosures regarding operating costs and Item 19 financial performance disclosures.

b. <u>Lead with Company-Operated</u>

In systems that have both company-operated and franchise locations, the brand may consider whether to launch delivery services via an aggregator at company-operated locations first. On one hand, this approach allows the franchisor to test and adjust delivery practices before launching them more broadly to the entire system. This approach may also allow the franchisor to demonstrate the benefits offered by the aggregator partnership to the rest of the system,

---

[16] Jennifer Dolman & Dominic Mochrie, *Driving Sales Without Driving You Crazy – The Unique Challenges of Delivery Aggregators in Franchise Systems*, WHO'S WHO LEGAL (Nov. 14, 2019), https://whoswholegal.com/features/driving-sales-without-driving-you-crazy--the-unique-challenges-of-delivery-aggregators-in-franchise-systems.

[17] Don Fox et al., *Food Delivery Service Issues: The Last Mile – Navigating the Restaurant Food Delivery Paradigm Shift*, INT'L FRANCHISE ASS'N 52ND ANNUAL LEGAL SYMPOSIUM (2019), https://www.franchise.org/sites/default/files/2019-05/FoodDeliveryServiceIssues.pdf.

[18] *See id.*

thereby increasing participation. On the other hand, this approach may not be well-received by franchisees who are eager to enter the delivery channel so that they may also reap the benefits and, potentially, generate increased sales that might otherwise be funneled to the franchisor during the company-operated soft launch.

c. Pilot Program

Brands may also consider adopting a “toe in the water” approach to partnering with an aggregator. Under this approach, the restaurant business partners with the aggregator for a limited time period and usually in a limited geographic area. This approach may be beneficial because it allows all sides to evaluate the aggregator model, including customer demand, product quality, delivery times, economic benefits and costs, and the level of partnership and support offered by the aggregator, before the parties commit to a full or long-term relationship. A pilot phase also allows all sides to adjust practices and ways of working based on the information gained during the pilot phase.

d. Determine Contracting Strategy

After deciding to move forward with partnering with an aggregator, restaurant franchise businesses should determine the strategy for approaching negotiations with the aggregator. One option is for the franchisor to lead negotiations directly with the aggregator with the goal of reaching an umbrella agreement that will apply to all stores interfacing with the aggregator platform, system-wide. This approach could be beneficial because it may give the brand more leverage, potentially resulting in better terms for all participants within the system. This may also be positive for franchisors and franchisees alike because the entire system would operate on the same set of contractual terms with the aggregator.

A second approach is to allow the franchisor to lead negotiations with the aggregator with the goal of reaching an agreement on a core set of terms that will be included in all agreements subsequently negotiated and executed by the aggregator and franchisees directly. Under this approach, however, there is risk that not all franchisees will receive the exact same terms in their agreements with the aggregator.

Finally, another approach may be for the franchisor to designate an aggregator as an approved supplier of digital delivery services and allow each franchisee to negotiate and execute its own agreement with the aggregator. This approach carries an even higher risk for different and varying terms within the system.

4. Anticipating Commonly Negotiated Issues

a. Exclusivity

As discussed above, aggregators are in constant competition with each other to attract and retain customers. One way that an aggregator can differentiate itself is by being the only platform where customers can make a digital delivery purchase for a certain popular restaurant or brand. Accordingly, aggregators often attempt to include exclusivity provisions in agreements with restaurant brands.

Franchise restaurant brands should carefully consider the benefits and risks of entering into an exclusive relationship with an aggregator. One potential benefit is that an aggregator may accept a lower commission rate in exchange for an exclusive relationship with the brand. A lower

commission rate can help preserve the profitability of orders placed via an aggregator and may make these relationships more palatable for franchisees. An aggregator may also consider offering a financial incentive in the form of reduced or waived delivery fees for customers of the brand.[19] This could also benefit the restaurant franchise business by driving value-seeking customers to the brand. The exclusive aggregator may also provide other benefits, such as prioritizing the exclusive brand in customer search results for particular types of food or providing advertising benefits of other kinds.

Another potential benefit to an exclusive relationship is that brands may find it more efficient to manage and administer a relationship with a single aggregator. This can be particularly helpful for restaurant operators because they will only need to interface with a single aggregator platform, including its hardware and software, rather than constantly juggling orders placed on multiple different aggregator platforms.

An exclusive relationship also has drawbacks. Obviously, by limiting the brand to interfacing with a single aggregator, the brand will not have access to customers that do not use that specific platform.[20] Accordingly, an exclusive relationship will restrict the brand's ability to access all potential customers. In addition, restaurant franchise businesses should be aware that, within the United States, each of the major aggregator players tends to have specific geographic areas in which the aggregator is most popular. Therefore, by entering into an exclusive relationship with an aggregator, the brand may be able to capitalize on the aggregator's success in one geographic region but may miss out on sales in other regions where the aggregator is less dominant.

A restaurant franchisor could consider placing limits on the scope of the exclusivity arrangement. For example, a brand may agree to an exclusive relationship with an aggregator, but only for a limited period of time or only in certain geographies. Of course, if a restaurant franchise business insists on placing limits on the scope of exclusivity, it should anticipate that the aggregator will correspondingly insist that any preferential financial terms offered by the aggregator only apply for the time period or geographic regions in which the exclusive relationship is in place.

In addition, a restaurant franchise business considering an exclusive aggregator relationship should consider in advance the potential effects when the exclusive relationship ends. As discussed above, it is likely that some preferential economic terms no longer apply after the end of the period of exclusivity. When those preferential terms sunset, there is risk that an aggregator could significantly increase the commission fee charged, creating an immediate negative effect on the profitability of sales made via the aggregator. Likewise, if customer-facing delivery fees increase at the end of the exclusivity period, this could drive customer traffic away from the brand, and potentially toward competitors that may be able to offer a better deal. A sudden and unexplained increase in fees payable by the customer could also negatively affect the brand's valuable goodwill among customers.

b. <u>Indemnity</u>

Indemnity is also likely to be a highly negotiated term in an agreement between a restaurant franchise business and an aggregator. Given that the aggregator handles ordering,

---

[19] *See* Goldstein, *supra* note 13.

[20] M. Houck, *supra* note 4 (noting exclusivity can restrict a brand's reach, relevancy, and revenue).

payment, and delivery, a restaurant franchise business may advocate for the aggregator to provide some form of indemnity protection for claims related to those services. These may include providing indemnity for claims related to the conduct of delivery drivers, claims related to restaurant data obtained by the aggregator, and claims related to customer information received by the aggregator.

However, aggregators may be extremely reluctant, or even completely opposed, to offering broad indemnity protection to restaurant franchise businesses. In particular, aggregators may be unwilling to offer indemnity protection for claims related to delivery drivers' conduct. This is because the business model of many aggregators relies heavily upon delivery drivers being treated as independent contractors under the law, where permitted. By treating drivers as independent contractors, rather than employees, aggregators reduce overhead costs like wages, payroll taxes, benefits costs, vehicle costs, vehicle maintenance and insurance costs, and gasoline expenses. If an aggregator were to offer indemnity protection for claims related to a driver's conduct, this could be construed by drivers, lawmakers, and litigants as a signal that the driver is actually an employee of the aggregator, exposing the aggregator to immense financial and legal risk.

c. Data

Restaurant franchise businesses should also prepare to negotiate terms regarding the use and ownership of data generated during the partnership with the aggregator. As an initial matter, the business should understand the various categories of data an aggregator may have access to in the course of the relationship. Aggregators likely receive information regarding customer name, the amount of the transaction, delivery location, and delivery time. It is also possible that the aggregator has access to additional information such as the specific menu items purchased, the customer's purchase history on the platform across other brands, brand loyalty program participation, reviews provided by the customer, and more.

Some aggregators take the position that all information received by the aggregator during the transaction is owned and controlled exclusively by the aggregator. Notably, this means that the aggregator now has access to extremely valuable information typically only accessible to the brands and restaurants – customer information. Accordingly, restaurant franchise businesses should consider negotiating, at a minimum, for the ability to access the data it deems most important for the brand and system. If the business does have access to, retain, or use any customer data, it should make sure that it has the right to do so pursuant to any aggregator terms of use and privacy policies and consider any additional legal implications, including relevant jurisdictions' privacy laws.

Restaurant franchise businesses may also consider requiring the aggregator to agree to some restrictions with respect to how the aggregator uses the data it receives by virtue of its relationship with the brand. For example, a restaurant franchise business could consider requesting a term preventing the aggregator from sharing such information with competitors. Or, a restaurant franchise business may advocate for a provision restricting the aggregator from using the information itself to compete directly with the restaurant franchise business.

d. Loyalty Programs

Franchise restaurant businesses should also consider negotiating terms relating to any existing brand loyalty program or aggregator loyalty program. If a brand has its own loyalty program, it may consider negotiating for terms requiring the aggregator to implement functionality

so that customer purchases made via the aggregator's platform integrate with the brand's existing loyalty program. Such integration may be difficult to achieve within the aggregator's existing technical environment, and integration could require significant investment or could simply be impossible. If integration is impossible, the brand should consider the potentially negative effect a lack of integration may have on the customer experience for the brand's loyalty program members. If an aggregator has its own loyalty program, the restaurant franchise business should understand how that program will be used when customers make purchases using the aggregator platform and any intersection that program may have with the brand's own loyalty program.

e. Service Standards

As detailed above, by entering into a relationship with an aggregator, a restaurant franchise business cedes some control over the customer relationship to the aggregator and the delivery drivers using the platform. Service provided by the aggregator and drivers in the "last mile" of the transaction can have a huge impact on the customer experience and, accordingly, the customer's satisfaction with the transaction and the brand as a whole. Therefore, restaurant franchise brands should consider requiring the aggregator to commit to some minimum service standards aimed at protecting the customer experience.

No delivery customer wants to receive food that is cold, soggy, or late on arrival. Restaurant franchise businesses may consider negotiating for a commitment that orders will be picked up by aggregator drivers within a certain average time period after the restaurant signals that the order is ready for pick-up. This may help ensure that the food is as fresh as possible when the driver arrives. Restaurants may also consider advocating for provisions aimed at protecting the quality of the food itself. For example, a restaurant may seek to include a provision or standard requiring that hot food items be transported in a container designed to retain warmth and cold items be stored in a cooler.

Restaurant franchise businesses may also consider negotiating for commitments relating to delivery times. One way to approach this is by requiring the aggregator to implement a system that allows customers to place orders only if the delivery location is no more than a certain distance away from the restaurant filling the order. Restaurants may also negotiate for commitments regarding the average time it takes for orders to be completed, measuring from the pick-up time to the time of delivery to the customer. Note that aggregators may resist making such commitments, arguing that many external variables outside of the aggregator's control can affect delivery time, such as weather, traffic, and road construction. Further, aggregators may argue that they cannot make any commitments on delivery times because they do not directly control the conduct of independent contractor delivery drivers.

Restaurant franchise businesses may also consider including provisions or mutually-agreed upon extra-contractual policies regarding how customer service issues will be handled between the aggregator, the franchisor, and the franchised location. Such provisions could address in advance how the parties inform each other of customer complaints received during the course of a digital delivery transaction. Provisions could also address in advance how customer complaints will be remedied. It may make sense for the party receiving the complaint to respond directly to the customer and to attempt to resolve the issue, regardless of whether the issue occurred when the responding party was in control. It could also make sense for the complaint to be forwarded to the party in control when the customer service issue arose and then to allow that party to resolve the issue. In either case, having a customer service redress process in place will help resolve customer issues more quickly and can help establish a culture of communication and accountability within the partnership.

Restaurant brands themselves can also take proactive steps to preserve quality in a delivery transaction. A brand might decide that certain products do not travel well and, therefore, voluntarily remove such items from the scope of items available for purchase on a platform.[21] Restaurants can also help preserve the quality of the end-product by selecting packaging for delivery transactions that transports well, results in minimal spillage, and retains the desired temperature. Finally, restaurants may also consider packaging delivery orders in tamper-proof packaging to give customers additional assurance regarding the food arriving at their doorstep.

5. Updating Franchise Agreements and Disclosure Documents

Entering into an arrangement with a third-party aggregator requires franchisors to carefully consider how the arrangement impacts existing and new franchise agreements and franchise disclosure documents. At a minimum, franchisors should consider updating those documents to reflect developments with respect to the scope of rights granted to franchisees, limitations on the protected territory (if any) granted to franchisees, the method for calculating royalties, and rights with respect to platform access.

a. Scope of Rights

Franchise agreements define the scope of franchisees' rights under the agreement and the rights reserved to the franchisor. Commonly, restaurant franchise agreements specifically state that franchisees can only make sales at approved physical restaurant locations and that franchisees cannot sell products through online sales, e-commerce, or other electronic platforms. A restaurant franchise business seeking to allow franchisees to enter the digital delivery channel should confirm whether its agreements contain these common provisions. If so, the agreements and description of rights set forth in franchise disclosure documents need to be updated to reflect that sales can be made via approved electronic platforms and whether participating in those types of sales can be mandated by the franchisor.

b. Exclusive Territory and Encroachment Considerations

Franchisors should also carefully consider how partnering with an aggregator could impact exclusive territories granted within existing franchise agreements. A typical exclusive territory provision may simply state that the franchisor will not place other restaurants operating under the same brand within the exclusive geographic territory granted to the franchisee. If the provision in question follows this structure, then the franchisor has at least three approaches to consider.

First, the franchisor could arguably take the position that sales made via an aggregator do not violate the exclusive territory provision because no physical store location has been placed inside the protected geographic territory. Of course, this position may expose the franchisor to risk of a claim because the aggregator relationship arguably deprives the franchisee of the ability to enjoy the benefit of the exclusive territory provision because other franchisees could fill orders for delivery to customers located within the franchisee's exclusive territory.

Second, the franchisor could seek to incentivize franchisees to modify existing exclusive territory provisions to carve-out sales made via the aggregator platform. Such a provision might leave the exclusive territory largely intact but include language limiting the scope of exclusivity to exclude sales made via an aggregator platform to customers located within the franchisee's

[21] There may be other reasons to remove a specific product from an aggregator platform, such as reducing sales tax complexities associated with sales of certain products.

exclusive territory. To succeed, this approach requires wide adoption throughout the system, which could be challenging to achieve and coordinate.

A third alternative is for the franchisor to negotiate terms with the aggregator requiring it to adjust its platform to consider existing exclusive territories within the system. An aggregator may be able to build information regarding exclusive territories into its algorithm and create a pathway for routing an order placed for delivery within a certain geographic area to the specific franchisee operating within that exclusive geographic territory. However, not all aggregators can or are willing to accommodate such complex and potentially resource-intensive back-end work.

c. Royalty Calculation

Franchisors should consider including provisions regarding how royalties payable by franchisees to the franchisor will be calculated on sales placed through the aggregator platform. As previously discussed, aggregators typically charge individual restaurants a commission equal to a certain defined percentage of each sale. Therefore, franchisors must decide whether the royalties payable under the franchise agreement are calculated on the total amount of the sale, including the commission charged by the aggregator, or whether the commission charged by the aggregator should be excluded from the amount of sales upon which the royalty due to the franchisor is calculated. Franchisors should clearly articulate this position in franchise agreements and other relevant documents to avoid uncertainty and confusion among its franchise base as well as to reduce the risk of potential legal claims.

d. Platform Access

Franchisors requiring participation in digital delivery platforms may also consider including provisions in franchise agreements that will make it a default of the agreement if a franchisee fails to participate in the program. Franchisors may also consider including a provision in franchise agreements allowing them to unilaterally remove a franchisee's access to a digital delivery platform in the event of an uncured default and, at a minimum, upon termination or expiration of the franchise agreement.

D. Mounting Tension

Demand for digital delivery services together with staggering projections on the potential growth of the channel make partnering with aggregators quite attractive. But, even if aggregators, franchisors, and franchisees can successfully navigate the contractual hurdles described above, there are many other obstacles the parties could face during the course of the relationship. The following sections examine some common obstacles and issues the parties may encounter during the course of the relationship and provide suggestions on overcoming them.

1. Disintermediation

A brand's relationship with its customers is critical to its survival. While restaurant franchise businesses pursue relationships with aggregators to attract and retain customers, there is also a risk that through partnering with an aggregator, the brand simply becomes an intermediary in the transaction. In this scenario, no longer is the primary customer relationship between the restaurant and the customer. Instead, the primary relationship is between the customer and the aggregator that controls the platform the customer turns to time and time again to search for food options, compare prices, and place orders. The brand and the individual restaurant location become nothing more than a middleman in the transaction between the

customer and the aggregator. This phenomenon is known as "disintermediation" and could obviously prove quite dangerous for restaurant franchise businesses.[22]

The prevalence and impact of disintermediation within the digital food delivery channel is not yet widely understood. As the channel grows and more brands enter into arrangements with aggregators, perhaps data will reveal whether disintermediation is a true threat to restaurant brand power or if it is just another obstacle restaurant franchise businesses need to overcome through other means.

Combating disintermediation is no easy task. However, there are steps restaurant franchises can take now to prevent themselves from becoming an intermediary in their own customer relationships. First, restaurant franchise brands could consider developing and maintaining their own platform that allows customers to view menus, place orders, and make digital purchases. This, of course, requires significant time, know-how, and a major financial investment, making this option inaccessible for most. But, if resources allow, developing a platform that allows brands to continue having a direct digital relationship with customers can certainly help reduce the impact of disintermediation. Panera Bread is one brand that successfully developed its own platform, but even it ultimately partnered with aggregators.[23] Other more traditional and less resource-intensive options exist for overcoming the disintermediation threat, such as brand-focused marketing campaigns on and off the platform, brand loyalty programs, and customer incentives targeted at driving customers to the brand more broadly.[24]

2. <u>Competition from Aggregators</u>

Restaurant franchise businesses are accustomed to operating in a competitive environment where restaurants compete directly against each other to attract customers and generate sales. In an aggregator arrangement, however, competition exists not only from other restaurants both on and off aggregator platforms, but competition also exists with the aggregator itself. Interestingly, some aggregators themselves are beginning to develop and operate their own food businesses that will market and sell food directly to customers using the platform.

Unlike traditional restaurant franchise businesses, however, these aggregator-operated concepts do not have a physical location that customers can visit to dine in or pick up food. Instead, the concept exists entirely on the platform and food is prepared in a food-preparation facility, known as a "dark kitchen", a "ghost kitchen", a "cloud kitchen", or a "delivery-only kitchen."[25]

Dark kitchens offer many advantages. These operations do not require a physical location that needs to welcome customers and provide seating. They do not even require a customer-facing storefront at all. Accordingly, dark kitchens require a smaller up-front investment in rent or

---

[22] *See* Goldstein, *supra* note 13.

[23] *See id.*

[24] *See id.*

[25] Isabelle Hanet, *What Is a Dark Kitchen?*, DELIVERECT (Sept. 2, 2019), https://www.deliverect.com/blog/dark-kitchens/what-is-a-dark-kitchen.

real estate.[26] In addition, labor costs can be significantly less in a dark kitchen concept. Dark kitchens only require back-of-the-house food staff and, potentially, a manager to orchestrate operations.[27] Therefore, dark kitchen operators can reap significant cost savings in terms of labor costs associated with front-of-the house employees like waitstaff or cashiers, which could enable them to beat traditional brands on prices for similar foods. Dark kitchens also require less investment in other items such as marketing outside of the platform, point-of-sale hardware and software, security systems, fixtures, furnishings, equipment, and general maintenance costs.

Another potential advantage of a dark kitchen is added flexibility. For example, a single dark kitchen can be used to prepare foods for multiple concepts. The flexibility of being able to operate multiple concepts out of a single commissary can amplify cost savings associated with dark kitchens because the operator can invest in a single set of pared-down resources while simultaneously attracting a broader set of customers across concepts. Similarly, dark kitchens can create flexibility to innovate and test new items and ways of working.[28] Without a customer-facing storefront, dark kitchen operators can easily change menu items and food offerings. Food preparation techniques and equipment can be reconfigured quickly and with minimal disruption to the overall business.

Deliveroo and Uber Eats have both tested dark kitchens.[29] Considering the deep pockets of some aggregators, the ability for dark kitchens to be used cost-effectively to operate multiple concepts, and the troves of customer data regarding customer habits and preferences accessible to aggregators, direct competition from aggregators could be fierce. Restaurant franchise business should, at a minimum, be aware of the risk that the aggregator could operate its own dark kitchens on the platform and consider negotiating for protections that prohibit the aggregator from competing directly with the brand or that prohibit the aggregator from using the brand's customer data to compete against it through dark kitchens.

3. <u>Prepare for Platform Access Issues</u>

Restaurant franchise businesses should also develop proactive strategies to address platform access issues that may arise in the course of the relationship. As an initial matter, the parties should develop a plan for efficiently onboarding participating franchisees as they either join the digital delivery program or open their first physical location. The parties should also align on the process for the franchisor to notify the aggregator when a franchised location should be removed from the platform whether due to ongoing default, closure, or termination. In addition, the parties should be aware that there could be circumstances when the aggregator may want to remove a franchised location from the platform due, perhaps due to a franchisee's alleged failure to properly engage with the platform. Franchise restaurant businesses should consider requiring the aggregator to give notice of any such violations both to the franchisor and franchisee before any removal from the platform and to offer the franchisee a reasonable time to cure the issue.

---

[26] *See id.*

[27] *See id.*

[28] *See id.*

[29] *See* Isaac et al.*, supra* note 10.

4. Consolidation

Following the birth of the digital delivery channel, the number of aggregators has steadily increased. In some geographies, the aggregator marketplace has become extremely crowded and competition among aggregators to attract and retain customers has intensified. To meet investor appetite for growth, aggregators commonly gobble up the competition through acquisitions of other aggregators.[30]

In 2016, JustEat acquired four other digital delivery businesses.[31] In recent years, Grubhub also acquired several companies operating in the related mobile order and loyalty channels.[32] Then, in a somewhat stunning announcement, in 2020, JustEat announced its acquisition of Grubhub for more than $7.3 billion dollars.[33] Conversely, in markets where a platform has not been successful, aggregators have sometimes simply exited the market altogether.[34]

Restaurant franchise businesses should take note of heavy consolidation in the aggregator industry. If a restaurant business chooses to partner with an aggregator that is later acquired by a competitor, the restaurant may find itself doing business with an aggregator the restaurant deems less suitable. This can be all the more difficult to swallow if the acquisition affects the standards, policies, and procedures previously agreed by the restaurant franchise business and the target aggregator. In other cases, a restaurant franchise business could find that the aggregator it partnered with and entrusted to develop its digital delivery business plans to close, potentially leaving the restaurant without access to the digital delivery channel for a time. An abrupt platform closure could also leave the restaurant business without access to customers who developed a routine of accessing the brand through the platform. If the business lacks access to customer data for these transactions, it may have no way of easily reconnecting with these customers. In light of the very recent history of significant consolidation within the aggregator industry, restaurant businesses should carefully consider change of control, assignment, termination provisions, and post-termination obligations within aggregator agreements.

5. Legal Developments

Restaurant franchise businesses pursuing the digital delivery channel through an aggregator should also track developments in state and local law relating to aggregators. At the state level, in early 2020, California introduced the Fair Food Delivery Act, targeted at protecting restaurant businesses from certain common aggregator business practices, including adding restaurants to a platform without consent and withholding customer data.[35] Since introduction, of the Fair Food Delivery Act, certain provisions requiring aggregators to share certain types of

---

[30] *See* Serene Chen, *On-Demand is Hungry for Marketshare*, STARTUPS VENTURE CAPITAL (Nov. 12, 2017), https://startupsventurecapital.com/the-hunger-games-on-demand-food-61029d955a6d.

[31] *See id.*

[32] *See Grubhub History*, GRUBHUB, https://about.grubhub.com/about-us/company-timeline/default.aspx (last visited June 19, 2020).

[33] *See* Cara Lombardo, Dana Cimilluca, & Ben Dummett, *Grubhub to Combine with Just Eat Takeaway.com in All-Stock Deal*, WALL STREET J. (June 10, 2020), https://www.wsj.com/articles/just-eat-takeaway-com-nears-all-stock-deal-for-grubhub-11591797653.

[34] *See* Mike Isaac & Kate Conger, *Uber Said to Be in Talks to Acquire Grubhub*, N.Y. TIMES (May 12, 2020), https://www.nytimes.com/2020/05/12/technology/uber-grubhub-deal.html.

[35] FAIR FOOD DELIVERY ACT, Assemb. B. 2149, 2019-2020 Leg., Reg. Sess. (Cal. 2020).

customer data with participating restaurants have been removed from the bill, perhaps signaling at least a preliminary victory for aggregators.[36] At the local level, as the COVID-19 crisis emerged, causing restaurants to close their dining rooms and spurring customers to turn to digital delivery, some municipalities introduced rules limiting the commission rate that aggregators can legally charge.[37] Restaurants should closely monitor this legislation and other similar legal developments as they might provide restaurant franchise businesses with additional rights and protections that do not exist within the four corners of the agreement with the aggregator.

6. Emerging Technologies

New technologies within the digital delivery industry are likely to compound the disruption associated with the rise of the channel. Already, aggregators are testing new technologies to deliver food to customers. Some businesses are reportedly testing drone autonomous delivery in certain markets.[38] Other businesses are beginning to use autonomous delivery vehicles, more commonly known as "robots", to make routine deliveries in closed environments like college campuses or office parks.[39] Forward-thinking restaurant franchise businesses will be prepared for the next wave of delivery technologies.

III. DATA PRIVACY AND PROTECTION

A. Understanding the Landscape

The evolution of technology creates a constantly shifting landscape for franchisors, as well as franchisees, especially in the area of privacy because franchisors collect information from franchisees and franchise candidates for a variety of purposes.[40] Aside from franchising, much of our information, even our face, is now data that is collected, stored, and used on a daily basis. Personal characteristics, habits, and opinions have become the most precious commodity out there. And in many cases, we have no idea how our information is collected, who is collecting it, or how it will be used. Even those collecting the information may not know exactly what they are collecting and how they will use it, even though they should.

1. Technology has caused more data to be collected

Gathering and using personal data is not a new concept, just more prevalent. From the first mainframe computer in the 1960s, data was collected and used by corporations to analyze information such as individual purchasing habits. In 1967, President Lyndon Johnson proposed a

---

[36] *See id.*

[37] Gabe Guarente, *Seattle Issues Emergency Order to Cap Delivery App Fees for Restaurants at 15 Percent*, SEATTLE EATER (Apr. 24, 2020), https://seattle.eater.com/2020/4/24/21235317/seattle-emergency-order-cap-restaurant-delivery-app-fees-15-percent; Bobby Allyn, *Restaurants Are Desperate – But You May Not Be Helping When You Use Delivery Apps*, NATIONAL PUBLIC RADIO (May 14, 2020), https://www.npr.org/2020/05/14/856444431/cities-crack-down-on-food-delivery-app-fees-as-restaurants-struggle-to-survive (noting that both Washington, D.C., and New York City passed similar rules).

[38] M. Houck, *supra* note 4.

[39] Singh, *supra* note 14.

[40] Franchisors use many different pieces of data such as a franchisee's name and address in a franchise application submitted online to ordering products. Meredith Fuchs and David L. Koch, *What Hath Technology Wrought? Franchisor Survival Guide to Online Privacy*, 19 FRANCHISE L.J. 47 (1999).

National Databank but Congress objected, stating that the data bank could "pool statistics on millions of Americans... and possibly violate their secret lives."[41] Legislators were so worried, in fact, that in the 1970s they created two federal advisory groups – the Automated Personal Data System (the "APDS") Committee and the Privacy Protection Study Commission (the "PPSC").[42] The concepts and ideas generated from these two groups culminated in the Federal Privacy Act of 1974, which provided protections against the federal government controlling medical data systems. Then came the first disruptor – the world wide web. Medical professionals soon realized the capabilities that the internet provided and invested millions to develop technology to harness the internet's power. The public and media started to scrutinize how medical records were used and discuss possible abuse. These concerns led then President Bill Clinton to propose the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")[43], calling it the "most sweeping privacy legislation ever written", and others to describe it as "staggeringly complex".[44] Since gathering medical data and personally identifiable information ("PII") first "became a thing", internet-based technology has evolved in many ways that enable franchisors to gather data and use it for the benefit of the franchise system in four different areas that we will explore in this section of the paper: (1) Marketing; (2) Loyalty Programs; (3) Customer Service/Retention; and (4) Financial Analysis/Reporting.

2. Uses and Benefits of Data in Franchise Systems

Franchisors use data to understand whether the goods or services they offer are in demand, learn about their customer base, devise ways to increase sales to their customer base and attract new customers. Franchisees benefit from the franchisor's collection of this data by gaining insights into the business without collecting and analyzing the data on their own. Franchisors use data gathered from their franchisees not only to obtain the foregoing insights, but also to understand how franchisees are performing and why some perform better than others. For those reasons, many franchisors are requiring their franchisees to submit data regarding their operations and customers to the franchisor on a regularly scheduled basis and prescribing the information that must be shared to gain the most comprehensive view of the franchised business's operations from the most franchisees possible.[45]

---

[41] Louise Matsakis, *The Wired Guide to Your Personal Data (and Who Is Using It)*, WIRED BUSINESS (Feb. 15, 2019), https://www.wired.com/story/wired-guide-personal-data-collection/.

[42] Jeffrey R. Yost, *Reprogramming the Hippocratic Oath: A Historical Examination of Early Medical Informatics and Privacy*, *in* THE HISTORY AND HERITAGE OF SCIENTIFIC AND TECHNOLOGICAL INFORMATION SYSTEMS 50 (W. Boyd Rayward & Mary Ellen Bowden eds., 2004).

[43] Although HIPAA was signed into law by President Bill Clinton on August 21, 1996, many updates and additions have been made, most notably the HIPAA Privacy Rule enacted in December 2000 (which introduced Protected Health Information, or "PHI"), The HIPAA Security Rule enacted in February 2003 (which established national standards to protect PHI), and the Health Information Technology for Economic and Clinical Health Act ("HITECH Act", which required collectors of PHI, as "Covered Entities," to notify patients in the event of a data breach and for "Business Associates" of the Covered Entities to comply with HIPAA. *When was HIPAA enacted?*, THE HIPAA JOURNAL (Mar.9, 2018), https://www.hipaajournal.com/when-was-hipaa-enacted/.

[44] Yost, *supra* note 42, at 53.

[45] Dennis Hung, *How to Make Big Data Work for Franchises*, INNOVATION ENTERPRISE (June 9, 2019), https://channels.theinnovationenterprise.com/articles/how-to-make-big-data-work-for-franchises.

a. Marketing

Marketing methods have evolved as technology provides new ways to reach consumers. Because, at least until the early twentieth century, individuals produced much of what they needed or simply used limited, local choices for goods, marketing did not emerge until the competition increased for mass-produced goods and services in the 1920s. Even then, marketing techniques were mostly limited to undercutting prices, but marketers started to rely on radio and newspapers to deliver their message. To gauge the effectiveness of the marketing, George Gallup started the Audience Research Institute, and the field of marketing research was born.[46] In 1941, television changed the game with the first advertisement from Bulova Clocks, and by 1954, there were more television advertisements than magazine advertisements.[47] Marketers then expanded marketing to telemarketing as companies started to focus more on customer needs, and the customer became "king". The next game changer was not the birth of the computer, but the birth of the Mac computer, which was the most famous advertisement to air during the Super Bowl in the United States.[48]

In 1995, search engines[49] were invented and transformed how individuals obtain information about topics and the speed with which they could obtain that information.[50] Originally, individuals used search engines to obtain lists of documents. Now consumers use search engines to "solve problems, accomplish tasks and "do" something."[51] Google, for example, is now such a popular search engine that it processes 40,000 search queries every second, which is 3.5 billion searches per day and 1.2 trillion searches per year worldwide.[52] As you can imagine, marketers looked for ways to harness that power to reach consumers and found that consumers take a winding path through various information until they find what they need, and because of that, search has evolved from simply words on the page to understanding user intent at all the twists and turns, otherwise known as the "consumer journey".

But it gets more complex. Today's consumer may start a search at work on a computer, then continue that search on their smartphone, and finish on their Google Home. To keep up with consumers, markets have evolved search engine optimization ("SEO"), so that when a consumer types in a search, the search engine then focuses on understanding personas, data-driven insights, content strategy and technical problem-solving to touch the three major areas of

---

[46] *The Evolution of Marketing from Trade to Technology*, GETSMARTER (Feb. 4, 2019), https://www.getsmarter.com/blog/market-trends/the-evolution-of-marketing-from-trade-to-technology/ [hereinafter *The Evolution of Marketing*].

[47] *Id.* (reporting that Bulova Clocks paid $9 for a 20-second slot).

[48] Aaron Taube, *How the Greatest Super Bowl Ad Ever – Apple's '1984' – Almost Didn't Make it to Air*, BUSINESS INSIDER (Jan. 22, 2014), https://www.businessinsider.com/apple-super-bowl-retrospective-2014-1?IR=T.

[49] Search engines are software products that store, in a database, data they collect on a website, including a url, keywords and links to help users know the content that is included in the specific website. Young J. Yoon, Note, *Legal Ramifications of "Black Hat" Search Engine Optimization*, 20 B.U. J. SCI. & TECH. L. 159, 162 (2014).

[50] *The Evolution of Marketing*, *supra* note 46.

[51] In the words of Bill Gates, "the future of search is verbs". *See* Ryan Jones, *Why Search – and SEO – Is Important*, SEARCH ENGINE JOURNAL (Jan. 3, 2018), https://www.searchenginejournal.com/seo-101/why-is-search-important/.

[52] By way of comparison, in 1998, Google processed an average of 10,000 search queries per day. *Google Search Statistics*, INTERNET LIVE STATS, https://www.internetlivestats.com/google-search-statistics/#trend (last visited June 19, 2020).

marketing – attract, engage, and convert[53] through "white hat"[54] and not "black hat"[55] methods. Ultimately, the marketer's goal is to have a certain website appear in the top results of certain keywords. Now that the marketer directs you to a specific site, the search engine you used can harvest information about your activity and link it to other information about you.[56]

Franchisors can use SEO to find franchisee candidates who use a Google search to find franchises of interest and to maximize its visibility online by having a website ready with the information the potential franchisee seeks. SEO leads have a higher closure rate than direct mail or print advertising, and SEO costs less.[57] Madison Marketing asserts that "[b]y giving [the candidate] good information they went looking for, you immediately build trust and position your brand as a problem-solver—all before anyone picks up a phone."[58]

Franchisees, on the other hand, can use SEO to obtain and retain customers as consumers increasingly rely on SEO to find products and services. For example, if a customer types in an online search for carpet cleaners in Madison, Wisconsin, the franchisee wants to ensure that its business comes up in the search. However, to maximize the potential to convert the consumer to a customer, the franchisee should ensure that all the information the customer needs to make a decision is also available on the franchisee's website – location, pricing, description of the service, customer reviews and contact information.[59] Franchisors may want to keep a tight rein on franchisee web content and usage to prevent SEO practices that may adversely impact the brand.

b. <u>Loyalty programs</u>

Loyalty programs are another mechanism that companies use to attract and retain customers, but also a way to harvest data from the customers who participate. Loyalty programs

---

[53] "Good" search engines should focus on content, navigation, solving technical issues, and integration (with social media platforms, content, creative, user experience, paid search, and analytics).

[54] "White hat" SEO techniques include: creating "unique [and] accurate page titles;" making use of a "description meta tag;" improving the structure of the website's URLs; making the website easier to navigate; optimizing displayed images; using "heading tags appropriately;" and offering "quality content and services." Yoon, *supra* note 49 at 162.

[55] "Black hat" SEO consists of methods that take advantage of search algorithms to unfairly promote or demote certain rankings or, in extreme cases, ban a website from all search results. Specific "black hat" techniques may include content scraping, link spamming, cloaking, doorway pages, keyword stuffing, and link farming. *Id.* at 162-63.

[56] Chrome, for example, is a browser that can be linked to a Google account, so it can obtain information on you from "multiple angles." Sarah Meyer, *Data Privacy Concerns with Search Engines*, CPO MAGAZINE (Dec. 25, 2018), https://www.cpomagazine.com/data-privacy/data-privacy-concerns-with-search-engines/.

[57] Based on SEO statistics, Madison Marketing calculated that SEO leads have a 14.6% average close rate, while outbound leads (such as direct mail or print advertising) have a 1.7% average close rate. Madison Marketing also advises that obtaining leads through SEO cost 61% less to acquire than leads generated through outbound marketing, like direct mail, trade shows, and telemarketing. *Franchise SEO in 2020: How to Grow Existing Franchises and Find New Ones*, MADISON MARKETING (July 5, 2020), https://www.madisonmarketing.com/resource/how-to-grow-existing-franchises-and-find-new-ones/.

[58] *Id*.

[59] *Id*.

are not new but have certainly evolved in importance from the secret decoders of the 1930s.[60] In fact, as much as 64% of retailers believe loyalty programs are the best way to connect with customers.[61] Customers also expect and rely on loyalty programs to choose a source for a product or service, as well as to increase their savings on that product or service.[62] Unsuccessful customer loyalty programs can have the opposite effect, causing customers to abandon the program and in some cases, the retailer, because of (1) lack of reward flexibility; (2) lack of seamless multi-channel experience; and (3) customer service issues.[63]

Key characteristics of successful customer loyalty programs are: (1) outstanding rewards; (2) emotional connection; (3) digital optimization; (4) delivering a seamless and unique experience; (5) thinking beyond transactions; and (6) leveraging analytics. Outstanding rewards vary from cash back to discounts, perks, rewards, prizes, custom products, exclusives, and merchandise, all of which should be aimed at enhancing the brand experience and motivating customers to engage and interact with your brand. At the end of the day, customers "…want some kind of acknowledgment that they are indeed your best customers. Rewards are a component for driving customer loyalty because it makes them feel special and recognized by the companies they buy from."[64]

The landscape of customer loyalty programs has evolved with technology, causing customers to expect more digital experiences.[65] Investing in the latest technology and analytics has become a necessity, not a nice-to-have as customers expect seamless omnichannel experiences as well as rewards. Businesses are specifically looking at big investments in technology and telecommunication companies in artificial intelligence to help analyze mass amounts of data quickly to personalize customer initiatives and experiences, as well as, customer service chatbots[66] and application programming interfaces. Companies are also leveraging third

---

[60] David M. Byers et al., *Gift Cards and Loyalty Programs in Franchise Systems*, ABA 33RD ANNUAL FORUM ON FRANCHISING W-7, at 25 (2010).

[61] Stacey Rudolph, *Why Customer Loyalty Programs are Important for Your Business*, BUSINESS 2 COMMUNITY (Apr. 5, 2016), https://www.business2community.com/infographics/customer-loyalty-programs-important-business-infographic-01500553.

[62] 69% of customers say that loyalty programs influence their choice of retailer; 57% of customers say they want to save money; and 37.5% of customers say they want to receive rewards. A whopping 76% of customers believe that a loyalty program "deepens their relationship with brands". *Id*.

[63] 44% of customers abandon due to lack of reward relevance, flexibility, and value; 33% abandon due to lack of a seamless multi-channel experience; and 17% abandon due to customer service issues. Grace Miller, *4 Things The World's Most Successful Customer Loyalty Programs Have in Common*, ANNEX CLOUD (June 9, 2020), https://www.annexcloud.com/blog/4-things-the-worlds-most-successful-loyalty-programs-have-in-common/.

[64] HARVARD BUS. REVIEW ANALYTIC SERVS., PULSE SURVEY, BEYOND REWARDS: RAISING THE BAR ON CUSTOMER LOYALTY at 1 (2019).

[65] Now that customers can get a ride from Uber or another service on their smartphone, they want the same experience with customer loyalty programs. *Id.* at 4.

[66] Chatbots are computer programs that simulate a conversation with a human, either by voice or text. Chatbots can be used in smart speakers, smart home devices, and chat and messaging platforms such as SMS, Facebook Messenger, WhatsApp, and LINE. Natalie Petouhoff, *What Is a Chatbot and How Is It Changing Customer Experience?,* SALESFORCE BLOG (Apr. 25, 2019), https://www.salesforce.com/blog/2019/04/what-is-a-chatbot.html/.

parties to assist with the above and with the administration of the loyalty program generally.[67]

Running loyalty programs poses legal challenges because loyalty programs can involve so many areas of the law. Generally, loyalty programs that ensure the terms and conditions provided to the consumer include rights to modify the program, termination rights, and notice provisions,[68] are not unfair or deceptive.[69] Additionally, terms and conditions that specify whether program points or similar parts of the program expire or cannot be used after a certain time period,[70] and observe privacy and security laws are more likely to survive challenge.

Some new loyalty programs have added yet another feature, gamification. Gamification does not necessarily mean an actual game, but taking game elements, most often, points, badges and leaderboards, and applying them to a loyalty program.[71] Tim Hortons, for example, added gamification to its rewards program so customers earn prizes as they visit their restaurants more frequently.[72] Tim Hortons now offers an annual game to customers. However, its planned "Roll Up The Rim" contest which incorporated the use of physical cups initially, followed by digital play, was scheduled to begin in April 2020, but became all digital due to COVID-19 concerns.[73]

Some have expressed concerns that gamification of loyalty programs is a habit-forming design (e.g., drawing the user into compulsive behavior) that may actually be problematic for customers and brands. For example, Sean Parker, the inventor of Napster and later the first company president at Facebook, said designers of these programs have "exploit[ed] a vulnerability in human psychology" by "giv[ing] users 'a little dopamine hit'" when doing so would

---

[67] Harvard estimates 31% of companies allow a third party to manage the loyalty program and 28% use a third party to manage loyal marketing campaigns. HARVARD BUS. REVIEW ANALYTIC SERVS., *supra* note 64 at 7.

[68] Specifically, program terms should have a notice provision that defines: (1) how notice of changes will be provided; (2) how much notice will be provided; and (3) how members will accept changes. Melissa Landau Steinman et al., *Rewarding Compliance-Laws, Regulations, and Litigation Relevant to Complex Loyalty Programs*, ASSOCIATION OF CORPORATE COUNSEL, NAT'L CAP. REGION at 5 (Dec. 13, 2018), https://www.acc.com/sites/default/files/2019-03/12-1-3-18-Loyalty.pdf.

[69] The program cannot be promoted in a false or misleading manner, fail to disclose material terms and conditions conspicuously and clearly, or fail to meet consumer expectations and assumptions. *Id.* at 7.

[70] It is unclear whether loyalty program points, credits, accrued discounts, etc. will be treated as subject to the unclaimed property laws, but by including this information it is likely to satisfy escheat laws. *Id.* at 10.

[71] Points are rewards for individual actions to drive repeating desirable behaviors. Badges, on the other hand, mark "larger milestone achievements", and leaderboards track the status of all players. These gamification methods encourage eight marketing drivers: "Meaning – The desire to feel that actions have purpose Accomplishment – The drive to achieve and overcome challenges Empowerment – The desire to choose one's own direction and try a variety of solutions to a problem Ownership – The desire to own things and have possession Social Influence – The drive to interact with, help, learn from, and compete with others Scarcity – The drive of wanting things you can't have Unpredictability – The drive of wanting to know what will happen next Avoidance – The drive to avoid pain or negative consequences." C&EN Media Group, *Psychology of Marketing Gamification: What Works and What Doesn't?*, C&EN MARKETING ELEMENTS BLOG (Apr. 11, 2018) https://acsmediakit.org/blog/psychology-of-marketing-gamification-what-works-and-what-doesnt/.

[72] Blake Morgan, *20 Fresh Examples of Customer Experience Innovation*, FORBES (Oct. 21, 2019), https://www.forbes.com/sites/blakemorgan/2019/10/21/20-fresh-examples-of-customer-experience-innovation/#60c9483b7c41.

[73] *Tim Hortons' first-ever cup-less RRRoll Up The Rim To Win begins today*, DAILY HIVE (Mar. 11, 2020), https://dailyhive.com/vancouver/tim-hortons-roll-up-the-rim-begins-digital.

help the company "consume as much of [the users'] time and conscious attention as possible."[74] As gamification technology becomes more prevalent, regulators are attempting to require warnings and restrictions, perhaps as a deceptive practice or as gambling.[75] Children are especially vulnerable to games and arguably need protection in addition to the data privacy protection for children from the Children's Online Privacy Protection Act ("COPPA").[76] COPPA does require parental consent and restricts personal information that may be collected from the child[77], but does nothing to lessen the addictiveness of the game. For purposes of this paper we have focused only on the loyalty program as a disruptor, which is primarily in the area of data mining and which is discussed later in this paper.[78]

c. Customer Service / Retention

Customer Service is another area that has changed greatly from the days that customers visited their local mercantile and were personally served by the proprietor, with whom they could discuss any issues. Technological advances have made it possible to handle customer service issues remotely while, companies hope, preserving the personal service consumers desire.

Face-to-Face video has increased and now can be used to leave video voicemails or video conference. Video voicemails are short videos that companies can send via email to a customer to better connect, especially for situations that may require a more personal touch.[79] Now that people screen emails, studies have shown that if the word "video" is in the subject line of the email, customers are 19% more likely to read the email. Additionally, unlike leaving a voicemail, providing such messages via email allows a company to determine if the customer actually heard

---

[74] Kyle Langvardt, *Regulating Habit-forming Technology*, 88 FORDHAM L. REV. 129, 142 (2019).

[75] Langvardt found that in Google's Play Store and Apple's iTunes Store, although children's applications are found in the "Family" section, in some cases children using applications in the Family section have been "lured" into "apps that have parted them from their parents' money at casino-like rates of thousands of dollars per hour," thus demonstrating a conflict between the idea of a Family section and the developer's "aggressive monetization model". *Id* at 165.

[76] COPPA prohibits (1) a person operating a website or online service for commercial purposes such as offering products or services for sale through that website or online service ("online service provider" or "OSP"), or a person who, on behalf of the OSP, "collects or maintains personal information from or about the users of, or visitors to," such online services from (2) targeting or knowingly collecting personal information from children under the age of thirteen and unfair or deceptive acts or practices performed in connection with personal information from and about children on the internet. Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888 (Nov. 3, 1999) (codified at 16 C.F.R. § 312 (2012)). COPPA is enforced by the FTC in accordance with 16 C.F.R. § 312.

[77] COPPA incorporates five "Fair Information Practice Principles": (1) Notice; (2) Choice; (3) Access; (4) Security; and (5) Enforcement. Websites must include a notice containing what information is collected, how it is used, and its information disclosure practices. The OSP must obtain verifiable parental consent through reasonable efforts for the collection of the child's personal data and give the parent the ability to obtain a description of the personal information collected, obtain the personal information collected, and refuse to permit the collection of any additional personal information. Eldar Habar, *Toying with Privacy: Regulating the Internet of Toys*, 80 OHIO ST. L.J. 399, 416-420 (2019).

[78] Loyalty programs can involve the following areas of law: contract, UDAP/Consumer Protection, Gift Cards/Stored Value/Coupons, Privacy and Data Security, Sweepstakes/Contests/Charitable Promotions, Unclaimed Property/Tax, Money Transmission, Human Rights/Americans with Disabilities Act, Fraud, Social Media/FTC Endorsements & Testimonials Rule, Antitrust, Franchise and Third Party Agreements. *See* Steinman, *supra* note 68.

[79] Meryl Ayres, *Stand Out In The Inbox With Video Voicemails*, WISTIA (Sept. 8, 2016), https://wistia.com/learn/sales/stand-out-with-video-voicemails.

the message or whether it was deleted unopened.[80] Similarly, video conferencing, through software such as Zoom, enables a customer to interact with a customer service representative while maintaining eye contact to increase openness. The outbreak of COVID-19 made companies increase their usage of videoconferencing to connect with remote workers, customers, and employees. As a result, specific companies have experienced exponential growth,[81] even those that offered their services for free during the crisis.[82]

As previously mentioned in this paper, another development in customer service is the chat-bot. A chat-bot can reply to a customer, thus creating a back-and-forth conversation. Accenture believes the earliest example of a chat-bot was ELIZA, built in 1966, which was a program that responded to a user's typed questions by using a script and pattern-matching.[83] Whole Foods now uses a chat-bot to help customers chat with the bot to find new recipes and ways to use ingredients from the store, even enabling customers to send a food emoji to get a recipe for that food.[84] Chat-bots have arguably increased in popularity and importance due to the public's increase use of messaging platforms such as Whatsapp, Facebook Messenger, We Chat and LINE. Now a customer can make payments, order items, book restaurant reservations, and ask questions through a messaging app rather than in person or over the phone. Additionally, the emergence of artificial intelligence and machine learning allow companies to cheaply take advantage of mass amounts of data and predict customer needs.[85] As a result, these companies are able to improve decision-making and understanding of customer patterns, making chat-bots the go-to solution for specific areas of customer service where the solutions are well-known, predictable, and high in volume.[86] For example, Madison Reed uses chat-bots to recommend hair colors, and Cleo uses chat-bots to provide financial advice.

Of course, with the rise of the chat-bot has come a rise in litigation. The most recent case, *In re Equifax Inc. Customer Data Sec. Breach Litig.,*[87] in which Equifax attempted to settle litigation involving a data breach by sending notices to members of the certified class through email, newspaper, a digital and social media campaign, a special settlement website, and a toll-free number staffed by live operators where class members could ask questions about the

---

[80] Sati Hillyer, *Leave a Video, not a Voicemail*, ONEMOB (July 15, 2018), https://blog.onemob.com/making-voicemails-personal/.

[81] These companies include 8x8, Inc., Cisco Systems, Inc., Google LLC, Lifesize, Inc., LogMeIn, Inc., Microsoft Corp., RingCentral, Inc., StarLeaf Ltd., Zoho Corp. Pvt. Ltd., Zoom VideoCommunications, Inc. *Impact of COVID-19 on the Videoconferencing Market, 2020*, *ResearchAndMarkets.com*, BUSINESSWIRE (Apr. 16, 2020), https://www.businesswire.com/news/home/20200416005739/en/Impact-COVID-19-Video-Conferencing-Market-2020.

[82] *Id.*

[83] *Chatbots in Customer Service*, ACCENTURE INTERACTIVE at 3 (2016), https://www.accenture.com/t00010101T000000__w__/br-pt/_acnmedia/PDF-45/Accenture-Chatbots-Customer-Service.pdf.

[84] Morgan, *supra* note 72.

[85] ACCENTURE INTERACTIVE, *supra* note 83, at 7.

[86] *Id.*

[87] No. 1:17-MD-2800-TWT, 2020 WL 256132 (N.D. Ga. Mar. 17, 2020).

settlement.[88] 388 of the 147 million class members objected to the settlement.[89] The facts of the case revealed that a claims aggregator created a website, www.NoThanksEquifax.com, which used a chat-bot created by Class Action, Inc. to encourage class members to object to the settlement by using inflammatory and false and misleading language. In analyzing the validity of these objections in relation to the settlement, the court ruled that the objections were invalid as they were instigated by false and misleading information provided through the improper actions of Class Action, Inc.[90]

d. Data mining

In addition to better customer service, loyalty, and other technology programs that focus on the collection of customer data also track every transaction between a customer and a brand so that marketers can track the customer's buying habits, values, and lifestyle – information commonly referred to as "Big Data".[91] "Data Mining", a term coined in the 1990s, is the process of using Big Data to find anomalies, patterns, and correlations in consumer behavior to predict outcomes and, hopefully, improve customer relationships, reduce risks, and ultimately persuade the customer to continue to purchase, preferably, at a higher price point.[92] Data mining uses statistics, artificial intelligence, and machine learning to "discover relationships among everything from price optimization, promotions, and demographics to how the economy, risk, competition, and social media are affecting their business models, revenues, operations and customer relationships."[93] As processor speed increases, so does the marketers ability to use Big Data and Data Mining.

With the increased practice of Data Mining, comes increased scrutiny around the uses of the practice. For example, in 2018, it was revealed that a professor created an application that predicted personality based on an individual's Facebook feed, likes, and posts. The application not only captured information about the user's Facebook profile, but also the profiles of the user's friends. That information was then sold to Cambridge Analytica, which assisted the 2016 presidential campaign of Donald Trump in targeting users via social media.[94] Christopher Wylie, a political strategist who previously worked for Cambridge Analytica, stated during an interview with NBC's Today Show that Cambridge Analytica believes that if a company can "capture every channel of information around a person and then inject content around them, you can change their perception of what's actually happening" – a practice Wylie called "informational dominance".

---

[88] *Equifax*, 2020 WL 256132, at *4.

[89] *Id.* at *14.

[90] "Objectors to a class settlement or their attorneys may not communicate misleading or inaccurate statements to class members about the terms of a settlement to induce them to file objections or to opt out." *Id.* at *42 (*quoting* Manual for Complex Litigation (Fourth) § 21.321 (2004) at § 21.33).

[91] Andy Wood, *Big Data: The Secret Weapon Behind Loyalty Programs*, CHIEF MARKETER (Dec. 9, 2015), https://www.chiefmarketer.com/big-data-secret-weapon-behind-loyalty-programs/.

[92] *Data Mining: What it is and why it matters*, SAS (June 10, 2010), https://www.sas.com/en_us/insights/analytics/data-mining.html.

[93] *Id.*

[94] Aarti Shahani, *Facebook Admits Data Mining Firm Got Access to Millions of Users' Personal Information*, NATIONAL PUBLIC RADIO (Mar. 19, 2018), https://www.npr.org/2018/03/19/595018770/facebook-admits-data-mining-firm-got-access-to-millions-of-users-personal-inform.

Wylie went on to say, "[w]e just put information into the bloodstream of the internet ... and then watch it grow, give it a little push every now and again … like a remote control…It has to happen without anyone thinking, 'that's propaganda,' because the moment you think 'that's propaganda,' the next question is, 'who's put that out?'"[95]

Similarly, in the case of *Dyroff v. Ultimate Software Grp., Inc.*,[96] the defendant used, Ultimate Software, its interactive computer service to create the "Experience Project", a social networking website where users could share personal stories and experiences. User registration was anonymous to encourage users to "share more personal and authentic information without inhibition."[97] The site did, however, use Big Data on an anonymous level to recommend other groups the users could join. Unfortunately, some customers did not use the site for purely legal purposes. For example, one user, Wesley Greer, posted in the group "where can i [*sic*] score heroin in Jacksonville [*sic*], fl [*sic*]." The system then sent him an email when another user "Potheadjuice", Hugo Margenat-Castro, posted in the same group. Greer died after using the service to buy what he thought was heroin from another Margenat-Castro. Plaintiff Kristanalea Dyroff, Wesley Greer's mother, filed a complaint in San Francisco Superior Court, alleging, among other things, that the defendant's service was negligent in sending users alerts to posts within groups that were dedicated to the sale and use of narcotics.[98]

After removing the case to federal court, the defendant filed a motion to dismiss which was granted by the federal district court without prejudice. The plaintiff appealed, arguing that pursuant to the Communications Decency Act, the defendant was an information content provider because its recommendation and notification functions were "specifically designed to make subjective, editorial decisions about users based on their posts."[99] In analyzing whether the plaintiff cited a claim for relief, the court analogized to its holding in *Fair Housing Council v. Roommates.com, LLC.*[100] In *Roommates.com*, the website asked users discriminatory questions to match people looking for rooms with landlords. The court held that because Roommates.com was responsible for the offending content, which was the cornerstone of each user's online profile, namely the discriminatory questions, Roommates.com was liable for violation of the Fair Housing Act. However, in *Dryoff*, the court reasoned that the website was not responsible for the creation of the offending content, but instead that the offending content was published by the users when they used the site to search for illicit drugs. Because the defendant did not make suggestions regarding potential content of posts or contribute to unlawful or objectionable posts, but merely used content-neutral tools to create its website, the court held that the defendant was not

---

[95] Tracey Lien, *A data mining company allegedly used facebook to distort users' reality*, L.A. TIMES (Mar. 20, 2018), https://www.latimes.com/business/technology/la-fi-tn-facebook-information-dominance-20180320-story.html.

[96] Dyroff v. Ultimate Software Grp., Inc., 934 F.3d 1093, 1098 (9th Cir. 2019).

[97] *Id.* at 1094-95.

[98] Plaintiff alleged that defendant: "(1) allowed users to traffic anonymously in illegal, deadly narcotics and to create groups dedicated to their sale and use; (2) steered users to additional groups dedicated to the sale and use of narcotics; (3) sent users alerts to posts within groups that were dedicated to the sale and use of narcotics; (4) permitted users to remain active accountholders despite evidence that they openly engaged in drug trafficking and that law enforcement had undertaken related investigations; and (5) demonstrated antipathy toward law enforcement efforts to stop illegal activity on Experience Project." *Id.* at 1095.

[99] *Id.* at 1096.

[100] 521 F.3d 1157 (9th Cir. 2009).

responsible for how a user put that software to use.[101]

Following *Dryoff*, the Federal Agency of News, LLC ("FAN") sued Facebook alleging that it had violated the Communications Decency Act ("CDA"), among other laws, by shutting down FAN's account and removing its page from Facebook's website.[102] Facebook defended its actions by arguing that FAN, a Russia-based Internet Research Agency, had violated Facebook's terms and conditions. FAN alleged that Facebook used Data Mining to generate billions in income and thus should not be protected by the CDA, which protects providers and users of interactive computer services. However, because Facebook only used Data Mining for Big Data to direct users to content to generate revenue, the court, citing *Dryoff*, held that Facebook's Data Mining was "…akin to recommendations and notifications—are tools meant to facilitate the communication and content of others; they are not content in and of themselves."[103]

Based on the holdings of *Dryoff*, *Roommates,* and *FAN*, restaurant franchise businesses can be comfortable with using Big Data and Data Mining to improve their marketing to customers, so long as the Big Data being utilized is generated solely by the users without the franchisor steering the user to provide certain answers or data. This use will remain valid even if the franchisor or company is, based on its Data Mining, recommending content or other sites to the user.

e. <u>Information sharing between franchisor and franchisee</u>

Restaurant franchise businesses can also benefit from Big Data to help provide unit-level metrics, customize systems, and provide insights on how the system is doing as a whole. Taylor Bond, founder of Franalytics Group, stated that "franchisors have to communicate to franchisees how important this is…Your gut is better with data -- I believe in informed gut decisions. How companies use and manage data is critical to their survival. Franchisors need to understand that without data, their left flank is wide open."[104] Great Clips, for example, used Big Data to help analyze customer frequency, preferred hairstyles, and days/times the customer liked to visit. Instead of having that information in localized databases, Great Clips added that information to its systemwide cloud, and now any of their salons can gather anonymized customer data.[105] Further franchised restaurant businesses can use Big Data gathered from all units to help manage inventory predictions and discounts, as well as predict labor needs.

Traditionally, franchisors received self-reported data from franchisees and thus were unable to validate accuracy, and inconsistencies in the data made analysis difficult. By imposing a standard reporting system through point-of-sale ("POS") technology, franchisors are able to shorten the time period needed to extract and analyze data and, by standardizing the data

---

[101] *Ultimate Software*, 934 F.3d at 1098-1099.

[102] Fed. Agency of News LLC v. Facebook, Inc., 432 F. Supp. 3d 1107 (N.D. Cal. 2020).

[103] *Id.* at 1118 (internal citations and quotations omitted).

[104] Jason Daley, *The Franchise World Finally Gets The Whole 'Big Data' Thing*, ENTREPRENEUR (Jan. 8, 2016), https://www.entrepreneur.com/article/253837.

[105] *Id.* It is unclear from the article if the data used by Great Clips and its franchisees was anonymized. Before franchisors provide customers' data to their franchisees, the franchisor should consider whether doing so complies with applicable privacy laws.

obtained, do a deeper dive into the data to surface relationships, trends and become more predictive. In the area of inventory management, for example, POS data can help franchisors ensure franchisees have access to needed products, determine top-selling items, and alert franchisees when ingredients or other key items need to be replenished.[106] The power of a POS solution enables the franchisor and franchisee to keep their fingers on the pulse of the business, through periodic reporting and surfacing key performance indicators ("KPIs") such as sales, gross profit, number of transactions, historical trends, and when the location is most busy, which information helps with staffing up at key periods. POS systems have also evolved from merely providing KPIs to enable franchisors to provide digital ordering.[107] POS also enable franchisors to collect Big Data from customers, especially through loyalty programs. The data franchisors obtain from the POS can be used to send newsletters, coupons and even to address customer service issues.[108] Other factors franchisors and franchisees should consider today when obtaining a POS system are whether it is a cloud-based system and has third-party integrations so that the POS can be integrated with other systems, like accounting software, payment processors, delivery companies, and more.

As with other technologies discussed in this paper, dependence on POS is not without data privacy pitfalls. Sonic encountered this most recently in the case *In re Sonic Corp. Customer Data Sec. Breach Litig*.[109] In the *Sonic* case, in 2017 hackers breached the POS in Sonic's franchisee-owned restaurants by installing malware that enabled the hackers to skim credit card data from the franchisee's customers. Plaintiffs, payment card issuing banks, sued Sonic for damages resulting from the plaintiffs' efforts to remediate the effects of the breach. The facts of the case reveal that Sonic suffered a data breach of its corporate-owned restaurants in 2015, and a third-party reviewer warned Sonic that similar attacks could occur in the future unless changes to security were made. Sonic required its franchisees to pay into a cybersecurity and technology fund. Sonic also required, through its franchise agreement, for Sonic franchisees to use Sonic-approved vendors, including POS vendors and security technology vendors. Sonic controlled the selection of technology (which included pre-configured settings), and the implementation timeline of the new technology, forbidding franchisees to change before roll-out.

Despite the 2015 warnings, in 2017 at least 23% of the Sonic locations still used the Kitchen Display System, technology so old that manufacturers stopped pushing updates and security patches a decade earlier, and which did not include any anti-virus or malware software.[110] Additionally, Sonic required its franchisees to maintain certain settings permitting permanent remote access that enabled Sonic, or hackers, to access the franchisees' cardholder data environments. The cardholder data was not encrypted because the franchisees used an outdated system for that portion of payment processing. The access enabled the hackers to install malware on the franchisees' POS through the Kitchen Display System and gain unencrypted customer credit card data in a format the hackers could use to duplicate user information onto stolen

---

[106] Sean Barkulis, *Why Universal POS Technology Makes All The Difference In Franchising*, FAST CASUAL (Aug. 9, 2016), https://www.fastcasual.com/blogs/why-universal-pos-technology-makes-all-the-difference-in-franchising/.

[107] Reema Bhatia, *How to Find the Right POS System for Your Franchise*, FORBES (Aug. 29, 2018), https://www.forbes.com/sites/forbestechcouncil/2018/08/29/how-to-find-the-right-pos-system-for-your-franchise/#7204b3d95f0e.

[108] Barkulis, *supra* note 106.

[109] In re Sonic Corp. Customer Data Sec. Breach Litig., No. 1:17-md-2807, 2020 WL 3577341 (N.D. Ohio Jul. 1, 2020).

[110] *Id.* at *4.

payment cards or make online purchases, as well as to sell the payment card data online. The hackers continued to gather data unchecked for six months because Sonic set up alerts using an invalid email address. Sonic moved to dismiss the plaintiffs' claim of negligence. However, the court ruled in favor of the plaintiffs, holding because it was foreseeable to any reasonable person that due to the 2015 hack and the failure to implement updated technology throughout the Sonic system, another hack could occur.[111]

Based on the *Sonic* case, franchisors should thoroughly consider their possible liability for mandating specific POS and especially security protocols or software. If the franchisor becomes aware of any vulnerabilities, the franchisor should move quickly to resolve those vulnerabilities system-wide.

B. Legislative and Regulatory Disruptions

Franchising has a long history of legislation and regulations that cause the industry to change. After a public outcry against unethical practices attributed to franchisors, the first federal regulation of distributors came in 1956 in the Automobile Dealers Day in Court Act. However, that law addressed only inequities between automobile manufacturers and distributors.[112] The first federal franchising regulation from the Federal Trade Commission went into effect in 1979 (the "FTC Rule"),[113] and state regulations began with California in 1971.[114] The FTC Rule required franchisors to disclose certain "material facts" and prohibited certain behaviors deemed unfair or deceptive.[115] Thus, the disclosure document was born. Additional federal legislation, the Petroleum Marketing Practices Act, was passed to govern petroleum franchises in 1978 to regulate termination and non-renewal.[116] States also passed legislation governing automobile dealerships and business opportunities.[117] This framework of regulations requiring written disclosure of specific information to a franchisee prior to entering a franchise relationship, and governing when and how a franchisor can terminate or non-renew a franchise was, arguably, a major disruptor in franchising and continues today as the original FTC Rule, the PMPA and state regulations are periodically modified. For purposes of this paper, we will concentrate on more

---

[111] *Id* at *13.

[112] The passage of this legislation was triggered by the failure of several major automobile manufacturers and distributors and was intended to make bargaining power between the automobile manufacturers and the distributors more equal, as well as to limit the automobile manufacturers' right to terminate a distributor. David Gurnick and Steve Vieux, *Case History of the American Business Franchise*, 24 OKLA. CITY U.L. REV. 37, 54 (1999).

[113] Promulgation of Trade Regulation Rule and Statement of Basis and Purpose, 43 Fed. Reg. 59,614, 59,623 (Dec. 21, 1978) (to be codified at 16 C.F.R. § 436).

[114] Dan Oates et al., *A State's Reach Cannot Exceed Its Grasp: Territorial Limitations on State Franchise Statutes*, 37 FRANCHISE L.J. 185, 187 (2017).

[115] Gurnick, *supra* note 112, at 56.

[116] 55 U.S.C. § 55.

[117] In 1964, Puerto Rico passed a law to protect dealerships from termination and non-renewal. In 1970, California passed the California Franchise Investment Law, which required registration and disclosure similar to a securities offering. The states of Hawaii, Illinois, Indiana, Maryland, Michigan, Minnesota, New York, North Dakota, Oregon, Rhode Island, South Dakota, Texas, Virginia, Washington, and Wisconsin followed with their own regulations. Gurnick, *supra* note 112, at 57-59.

recent developments in the data privacy area.[118]

The era of legislation and regulation of the new technology of harvesting information about internet users caused George W. Bush to sign into law the Controlling the Assault of Non-Solicited Pornography and Marketing Act (the "CAN-SPAM Act") on December 16, 2003.[119] The CAN-SPAM Act required, among other things, users to be able to opt-out of messages from spammers and prohibit the spammer from collecting information about the user. To comply with the CAN-SPAM Act, marketers must: (1) include their physical mailing address at the bottom of an email; (2) tell recipients where the email is coming from by including the sender's name or business name; (3) include a subject line that reflects what is in the email; and (4) include a way for the recipient to opt-out of the mailing list and comply with any opt-out requests within ten days of request.[120] The FTC modified CAN-SPAM in 2008, to include the following: (1) an e-mail recipient cannot be required to pay a fee, provide information other than his or her e-mail address and opt-out preferences, or take any steps other than sending a reply e-mail message or visiting a single Internet Web page to opt out of receiving future e-mail from a sender; (2) the definition of "sender" was modified to make it easier to determine which of multiple parties advertising in a single e-mail message is responsible for complying with the Act's opt-out requirements; (3) a "sender" of commercial e-mail can include an accurately-registered post office box or private mailbox established under United States Postal Service regulations to satisfy the Act's requirement that a commercial e-mail display a "valid physical postal address"; and (4) a definition of the term "person" was added to clarify that CAN-SPAM's obligations are not limited to natural persons.[121] In 2019 the FTC reviewed the CAN-SPAM Act but concluded no modifications needed to be made.[122]

As discussed previously, email has become a critical piece of Big Data and a primary way that marketers can communicate with consumers. The CAN-SPAM Act required marketing teams not only to change the form of their email marketing, but also to provide opt-out systems for recipients and a way to comply within ten days. However, are consumers really getting less spam email? According to Jaime de Guerre, CTO of antispam vendor Cloudmark, CAN-SPAM was mostly a "flop" because "the attackers are so advanced in their threats, and it's so hard to detect where they are coming from."[123]

Another technology that utilizes data mining is the practice of 'geofencing", or creating a

---

[118] For a summary of international laws regarding data privacy through January 2019, *see Global Tables of Data Privacy Laws and Bills (6th Ed. Jan. 2019)*, WORLDLII (Jan. 31, 2019), http://www.worldlii.org/cgi-bin/sinodisp/int/other/GTMDPL/2019/1.html?query=Global%20Tables%20of%20Data%20Privacy%20Laws%20and%20Bills.

[119] 15 U.S.C. § 103.

[120] *CAN-SPAM Act: A Compliance Guide for Business*, FEDERAL TRADE COMMISSION (June 11, 2020), https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business.

[121] *FTC Approves New Rule Provision Under the CAN-SPAM Act*, FEDERAL TRADE COMMISSION (May 12, 2008), https://www.ftc.gov/news-events/press-releases/2008/05/ftc-approves-new-rule-provision-under-can-spam-act.

[122] Cynthia J. Larose, *Federal Trade Commission: No Changes to CAN-SPAM Rules*, NATIONAL LAW REVIEW (Feb. 13, 2019), https://www.natlawreview.com/article/federal-trade-commission-no-changes-to-can-spam-rules.

[123] Carolyn Duffy Marsan, *CAN-SPAM: What Went Wrong*?, NETWORKWORLD (Oct. 6, 2008), https://www.networkworld.com/article/2276180/can-spam--what-went-wrong-.html.

virtual "fence" around a geographic area to interact with users inside the boundary[124] by using wireless internet, cellular data[125], global positioning systems ("GPS") and/or radio-frequency identification ("RFID") technologies.[126] "Active" geofencing triggers a response from a device after the subject crosses the boundary, whereas "passive" geofencing pushes advertising and other information to the subject or monitors or pulls information about the subject once the boundary is crossed.[127] Now marketers can send pop-up advertisements to customers based on location, also called "location-based marketing", so that the advertisements are relevant based on the customer's proximity to a store, competitor or another specific point of interest. In fact, the practice of geofencing specific areas based on a competitor are called "geo-conquesting." Geo-conquesting allows the marketer to deliver a competitive offer to a customer based on the customer's proximity to a competitor.[128] Burger King took the art of geo-conquesting to a new level with its "Whopper Detour" campaign in 2018. Based on the geofence, Burger King enabled customers within 600 feet of a McDonalds to order a Burger King Whopper for one penny from Burger King's app. Dunkin' Donuts also experimented with geo-conquesting in 2014 by offering customers a coupon to customers who were near competitors.[129]

1. European Union General Data Protection Regulation (the "GDPR") as an initial privacy disrupter

One point that stands out about CAN-SPAM is that it did not significantly limit how Big Data is collected and sold. The European Union originally tried to limit how consumers' Big Data was collected, used and sold in the Data Protection Directive adopted in 1995 (the "Directive").[130] The Directive was built upon seven principles of The Organization for Economic Cooperation and Development's Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data created in 1980, namely (the "Directive 7 Principles"): (a) Notice – individuals should be notified when their personal data is collected; (b) Purpose – use of personal data should be limited to the express purpose for which it was collected; (c) Consent – individual consent should be required before personal data is shared with other parties; (d) Security – collected data should be secured against abuse or compromise; (e) Disclosure – data collectors should inform individuals when their personal data is being collected; (f) Access – individuals should have the ability to access their personal data and correct any inaccuracies; and (g) Accountability – individuals should have a means to hold

---

[124] Kaya Ismail, *The Power of Geofence Marketing*, CMS WIRE (Aug. 19, 2019), https://www.cmswire.com/digital-marketing/the-power-of-geofence-marketing/.

[125] It should be noted that telecommunications carriers are prohibited from using or disclosing a "customer's proprietary network information" ("CPNI"), for any purpose other than to deliver the telecommunications services. Bozeman v. Verison, 18-CV-6270L, 2018 WL 9538051 (W.D.N.Y. Aug. 13, 2018) (citing 47 U.S.C. § 222(f)). For more information regarding privacy law and surveillance, *see* Steven Chabinsky and F. Paul Pittman, *USA: Data Protection Laws and Regulations 2020*, ICLG.COM (June 7, 2020), https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa.

[126] Charles Harris, *Mending (Geo)fencing Concern*s, JD SUPRA May 29, 2019, https://www.jdsupra.com/legalnews/mending-geo-fencing-concerns-12309/.

[127] *Id*.

[128] *Id.*; Ismail, *supra* note 124.

[129] Robert Williams, *Burger King Trolls McDonald's with Geolocation Stunt*, MOBILE MARKETER (Dec. 5, 2018), https://www.mobilemarketer.com/news/burger-king-trolls-mcdonalds-with-geolocation-stunt/543581/.

[130] Council Directive 95/46/EC, 1995 O.J. (L 281) 31.

data collectors accountable to the previous six principles.[131] The Directive, however, was non-binding, and different laws regarding data protection proliferated among European countries, causing compliance to be varied and spotty. However, it did set the framework for the GDPR not only by the Directive's 7 Principles, but also by defining personal data[132] as well as requiring controllers outside of the European Union to comply.[133]

The speed of technology soon outstripped the Directive because it did not reach far enough to control how Big Data is stored, collected, and transferred and did not "harmonize" data privacy laws across Europe.[134] On the other hand, GDPR, which went into effect on May 25, 2018, governs the collection and use of data from any individual residing in the European Union, as well as any country that collects data from an individual who is in a country that is part of the European Union.[135] In short, GDPR requires, for any information that allows a living person to be directly or indirectly identified ("Personal Data"),[136] that is processed[137] by a Data Processor[138] as required by a Data Controller[139] to follow seven principles (the "GDPR Principles"):

(1) **Lawful, Fair and Transparent Data Processing** - process Personal Data lawfully, fairly and with transparency to the data subject;

(2) **Legitimate Purpose** - process Personal Data for legitimate purposes that are identified to the data subject at the outset;

(3) **Minimize Collection** - minimize the Personal Data collected and processed to the extent absolutely necessary for the purpose identified to the data subject at the outset;

(4) **Accuracy** - keep the Personal Data up to date and accurate;

---

[131] Nate Lord, *What is the Data Protection Directive? The Predecessor to the GDPR*, DATA INSIDER (Sept. 12, 2018), https://digitalguardian.com/blog/what-data-protection-directive-predecessor-gdpr.

[132] The Directive defines personal data as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." Council Directive 95/46/EC, art. 2(a), 1995 O.J. (L 281) 31, 38.

[133] Council Directive 95/46/EC, art. 4, § 1, 1995 O.J. (L 281) 31, 39.

[134] Andrew Rossow, *The Birth of GDPR: What Is It and What You Need To Know*, FORBES (May 25, 2018), https://www.forbes.com/sites/andrewrossow/2018/05/25/the-birth-of-gdpr-what-is-it-and-what-you-need-to-know/#3f0f2b0f55e5.

[135] Commission Regulation 2016/679, 2016 O.J. (L 119) 1 (repealing Council Directive 95/46/EC).

[136] Personal Data includes names, email addresses, ID numbers, IP addresses, location information, ethnicity, gender, sexual orientation, biometric data, religious beliefs, web cookies, RFID tags, political opinions and pseudonymous data. Pseudonymous data, or data replaced by artificial identifiers to make the data less identifiable but still enables the data to be analyzed and processed, is only at issue if it is "relatively easy" to identify someone from it. Ben Wolford, *What Is GDPR, The EU's New Data Protection Law?*, GDPR.EU, https://gdpr.eu/what-is-gdpr/ (last visited Aug. 31, 2020).

[137] "Processing" means any automated or manual action performed on the data, including collecting, recording, organizing, structuring, storing, using and erasing. *Id.*

[138] A "Data Processor" is a third party that processes data for a Data Controller. *Id.*

[139] A "Data Controller" is a person who decides "why and how" personal data will be processed. *Id.*

(5) **Limit Storage** - limit storage of the personally identifying data to the period that is necessary for the stated purpose;

(6) **Ensure Security, Integrity, and Confidentiality** - process Personal Data in such a way as to ensure security, integrity and confidentiality; and

(7) **Accountability** - hold the Data Controller accountable for GDPR compliance.

Additionally, GDPR applies to any company collecting Personal Data and has a presence in a European Union country, processes Personal Data of European Union residents, has more than 250 employees or fewer than 250 employees but whose data collection impacts the rights and freedoms of data subjects.[140] To ensure compliance with GDPR, companies must determine what data is being processed, how it is processed, who is processing it, if the data being collected and processed is Personal Data, if the data subject was adequately made aware their data would be collected, if the Personal Data collected is limited to what is absolutely necessary, provide a means for the Personal Data to be kept accurate, limit the storage of the Personal Data, and ensure the Personal Data is secure. Companies must also be prepared to support data subjects GDPR "right to be forgotten," as discussed below.

In addition to the challenge to understanding GDPR, compliance is expensive.[141] Failing to adhere to GDPR is even more expensive – penalties for non-compliance are up to 20 million Euros, or 4% of global annual turnover, whichever is higher.[142] The Information Commissioner's Office in the United Kingdom stated, in July 2019, its intention to fine Marriott International with one of the largest GDPR fines to date - more than 99 million Euros – due to Personal Data exposed in a 2018 incident possibly caused when Starwood hotels group information systems were compromised in 2014, before Marriott's acquisition of Starwood.[143] Information Commissioner Elizabeth Denham said that Marriott should still be accountable although the breach stemmed from an event occurring prior to Marriott's acquisition of Starwood, stating:

> The GDPR makes it clear that organisations must be accountable for the personal data they hold. This can include carrying out proper due diligence when making a corporate acquisition, and putting in place proper accountability measures to assess not only what personal data has been acquired, but also how it is protected…Personal data has a real value so organisations have a legal duty to ensure its security, just like they would do with any other asset. If that doesn't happen, we will not hesitate to take

---

[140] Michael Nadeau, *General Data Protection Regulation (GDPR): What You Need To Know To Stay Compliant*, CSO ONLINE (June 12, 2020), https://www.csoonline.com/article/3202771/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html.

[141] Bloomberg Businessweek suggested it will cost $7.8 billion for multi-national companies to comply with GDPR. Jeremy Kahn, et al., *It'll Cost Billions for Companies to Comply with Europe's New Data Law*, BLOOMBERG BUSINESSWEEK (Mar. 22, 2018), https://www.bloomberg.com/news/articles/2018-03-22/it-ll-cost-billions-for-companies-to-comply-with-europe-s-new-data-law.

[142] Rossow, *supra* note 134.

[143] *Statement: Intention to fine Marriott International, Inc. more than £99 million under GDPR for data breach*, INFORMATION COMMISSIONER'S OFFICE (Jul. 9, 2019), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/.

strong action when necessary to protect the rights of the public.

The amount of the intended fine demonstrates that the more egregious the conduct as determined under the GDPR, the higher the penalty.[144]

In December 2016, Price Waterhouse Coopers estimated U.S. based companies would spend $1-$10 million each to meet the GDPR requirements, including creating a data breach incident response plan,[145] hiring a data protection officer ("DPO"), modifying privacy notices, creating opt-in systems, and implementing the "right to be forgotten".[146]

The European Data Protection Supervisor defines a DPO as an officer of an organization whose primary role is to "ensure that her organisation processes the personal data of its staff, customers, providers or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules."[147] A DPO cannot be a controller of processing activities, a short-term employee or a contract employee, report to a direct superior unless top management, or not responsible for managing the DPO's budget. Under the GDPR, failure to appoint a DPO triggers a fine of up to 10 million Euros or 2% of total worldwide annual turnover.[148] On April 28, 2020, the Litigation Chamber of the Belgian Data Protection Authority (the "Belgian DPA") imposed a €50,000 fine on a company for appointing its Head of Compliance, Risk Management and Audit as the DPO, creating a significant conflict of interest between the individual's role as Head of Compliance and its role as DPO and the "serious negligence" of the company shown by the duration of the infringement and the company's lack of preparedness considering its core business activity was processing Personal Data on a large scale.[149] The appointment of a DPO is a very real disruptor in the industry and is also a difficult role to fill. Axios suggests that although more than 20,000 people have passed the International Association of Privacy Professionals' exam, there are still not enough certified privacy professionals to meet demand.[150]

Two critical parts of GDPR are obtaining the individual's consent to collection of Personal

---

[144] GDPR regulators base fines on the following: (1) the nature of the infringement, including how many consumers were impacted, how long the violation occurred, and the purpose of the data processing; (2) whether the infringement was intentional or negligent; (3) what actions were taken after the incident, including prevention of similar incidents in future; (4) the cooperation of the company with regulatory and authoritative entities following an incident; (5) whether the company has a history of data privacy infringements; and (6) the type of Personal Data and how it was used. Claire Robinson, *Why becoming GDPR compliant is important for franchise businesses*, APPROVED FRANCHISE ASSOCIATION (June 13, 2020), https://www.theafa.org.uk/blog/why-becoming-gdpr-compliant-is-important-for-franchise-businesses/.

[145] A discussion of data breach incident response plans appears *infra* in Section III.D.

[146] Rossow, *supra* note 134.

[147] *Data Protection Officer (DPO)*, EUROPEAN DATA PROTECTION SUPERVISOR (June 13, 2020), https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en.

[148] Paul Luehr et al., *Franchising in a Sea of Data and a Tempest of Legal Change: Franchise Laws and Regulations 2020*, ICLG.COM (Oct. 21, 2019), https://iclg.com/practice-areas/franchise-laws-and-regulations/6-franchising-in-a-sea-of-data-and-a-tempest-of-legal-change.

[149] Hunton Andrews Kurth LLP, *Belgian DPA Sanctions Company for Non-Compliance with the GDPR's DPO Requirements*, NATIONAL LAW REVIEW (May 6, 2020), https://www.natlawreview.com/article/belgian-dpa-sanctions-company-non-compliance-gdpr-s-dpo-requirements.

[150] Jennifer A. Kingston, *The Global Shortage of Privacy Experts*, AXIOS (Nov. 1, 2019), https://www.axios.com/privacy-expert-shortage-202eda9b-c8fa-4bd4-b1c1-11844812ab3e.html.

Data and the opt-in requirement. Consent is not required in certain cases, such as to fulfill a contract.[151] If consent is required, the GDPR provides that consent cannot be implied from "silence, inactivity, default settings, taking advantage of inattention or inertia, or default bias".[152] Pre-ticked boxes are "banned", and opt-out consent is viewed by the Information Commissioner's office as, essentially, a pre-ticked box. Instead, consent is only given by clear and affirmative action, such as: (1) signing a consent, especially on paper; (2) clicking an opt-in button or link online; (3) selecting a prominent yes or no option; (3) choosing technical settings or preference dashboard settings; (4) responding to an email requesting consent; (5) answering yes to a clear oral consent request; (6) volunteering optional information for a specific purpose (such as optional fields in a form); and (7) dropping a business card into a box (the old-fashioned way).[153] A GDPR tracker shows, as of June 13, 2020, 305 companies fined for failure to properly obtain consent as required by the GDPR.[154] The fines ranged from 118 Euros to a 50,000,000 Euro fine imposed on Google.[155]

Article 17 of the GDPR contains a new concept, the "right to be forgotten", which is the right of a data subject to have its Personal Data erased "without undue delay" if: (1) the Personal Data is no longer needed for the purpose for which it was collected; (2) the data subject withdraws consent; (3) the data subject objects to processing its Personal Data and such processing is not needed due to "overriding legitimate grounds"; (4) the Personal Data is unlawfully processed; (5) the Personal Data must be erased for compliance with a legal obligation; (6) the Personal Data was collected pursuant to the offer of information security services.[156] However, the Personal Data does not need to be erased if processing the Personal Data is necessary for: (1) freedom of speech; (2) compliance with a legal obligation; (3) public interest of public health; (4) archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 of the GDPR; or (5) the establishment, exercise or defense of legal claims.[157] If the Personal Data is made public, the Data Controller must take "reasonable" actions to erase such data, taking into account available technology and cost of implementation. The "right to be forgotten" then, is another difficult hurdle for franchisors, and any company, to implement, and is thus, a serious disruptor in scope and complexity. Reasonable steps the Data Controller must take are not clear, but at a minimum, franchisors should have a data retention policy, clear communication of the data retention policy to the data subject, mechanisms to

---

[151] Consent is not required if the Personal Data is obtained: (1) to fulfill duties or obligations in a contract; (2) to comply with a legal obligation; (3) to protect physical integrity or life; (4) to accomplish a task in the public interest, which is usually performed by public authorities such as government departments, schools and other educational institutions; hospitals; and the police; (5) for genuine and legitimate reasons of an organization, even commercial benefit, as long as collection of the Personal Data is not outweighed by negative effects to the data subject's rights and freedoms. Luke Irwin, *GDPR: When Do You Need to Seek Consent?*, IT GOVERNANCE (May 7, 2020), https://www.itgovernance.eu/blog/en/gdpr-when-do-you-need-to-seek-consent.

[152] *Id*.

[153] *Id.*

[154] *GDPR Enforcement Tracker*, CMS, https://www.enforcementtracker.com/ [hereinafter *GDPR Enforcement Tracker*].

[155] Google's fine was imposed by the French data protection authority, the Commission Natonale de l'Informatique et des Libertés (the "CNIL") "for creation of a Google account during the configuration of a mobile phone using the Android operating system" that the CNIL determined violated GDPR because, among other things, the obtained consents were not "specific" and "unambiguous." *Id.*

[156] Commission Regulation 2016/679, art. 17, § 1, 2016 O.J. (L 119) 1, 43-44.

[157] Commission Regulation 2016/679, art. 17, § 3, 2016 O.J. (L 119) 1, 44.

remove Personal Data after the data retention period, a system to control dissemination of Personal Data to other Data Controllers, rules and regulations for any employees and third parties who process Personal Data, and a process for the Data Controller to inform other Data Controllers and Data Processors of an erasure request.[158] Right to be forgotten fines are not as numerous as opt-in fines; in fact, the GDPR Enforcement Tracker only shows eight fines ranging from 1,000 to a 75,000 Euro fine against Equifax Iberica S.L.[159]

Franchisors and franchisees may be viewed as joint Data Controllers of Personal Data depending upon whether each uses the Personal Data differently. For example, franchisors may use the Personal Data to determine which of the brand's products or services are best-sellers among different groups of individuals, whereas franchisees may use the Personal Data to send actual targeted marketing to individuals. Franchisors should remember that the obligations regarding Personal Data collection do not apply just to consumers of the brand's products or services, but also to the collection of Personal Data associated with marketing the franchise itself, as previously discussed in this paper.[160]

The GDPR strongly recommends Data Controllers perform a Data Protection Impact Assessment ("DPIA"), to determine the following:

> (1) A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; (2) An assessment of the necessity and proportionality of the processing operations in relation to the purposes; (3) An assessment of the risks to the rights and freedoms of data subjects; and (4) The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR, taking into account the rights and legitimate interests of data subjects and other persons concerned.[161]

So when performing their DPIA, franchisors should not forget to review the Personal Data as well as the franchise performance data the franchisor may use to sell franchises to any European Union residents.

2. <u>California Consumer Privacy Act (the "CCPA") adding onto the issue</u>

The CCPA is the newest privacy law that went into effect on January 1, 2020 and arguably,

---

[158] Sara Piron, *What does the GDPR 'right to erasure' mean in practice?*, LEXOLOGY (Apr. 3, 2018), https://www.lexology.com/library/detail.aspx?g=5976bed5-0f85-47cd-8484-34cdd76df703.

[159] Equifax Iberica claimed the data subject's request for erasure was excessive due to a prior request, but the Spanish Data Protection Authority deemed the denial a violation of the GDPR. *GDPR Enforcement Tracker*, *supra* note 154.

[160] *See* Irwin, *supra* note 151 for situations where consent is not needed.

[161] *Data Protection Impact Assessment*, GDPR.EU (July 6, 2020), https://gdpr.eu/data-protection-impact-assessment-template/. Use the following link for the actual template: https://gdpr.eu/wp-content/uploads/2019/03/dpia-template-v1.pdf.

the most far-reaching privacy law in the United States.[162] California lawmakers cited the Cambridge Analytica issue as justification for passing the CCPA.[163] The CCPA applies to "Covered Businesses", which are defined as any business having more than $25 million in revenue or buys and sells the Personal Data of 50,000 or more consumers in the State of California or derives 50% or more of its annual revenues from selling Personal Data.[164] The CCPA covers five basic areas:

(1) **Consumer Right to Know** – similar to the GDPR, consumers have a right to know what Personal Data is collected, sold, or otherwise disclosed, and Covered Businesses must comply with "verifiable requests" from consumers for this information;

(2) **Consumer Right to Delete** – similar to the GDPR's "right to be forgotten", consumers may request their Personal Data be deleted, and again, Covered Businesses must comply with verifiable requests for deletion unless maintaining the Personal Data is needed to consummate a transaction or provide a good or service;

(3) **Consumer Opt-Out** – California consumers can opt-out from the sale of their Personal Data, and Covered Businesses must (a) provide a clear and conspicuous hyperlink entitled "Do Not Sell My Personal Information" on their websites, (b) provide methods for consumers to opt-out of the sale of that consumer's Personal Data, including a website and toll-free number, and (c) honor all opt-outs and not contact a consumer who opted out for at least twelve months before seeking re-authorization to sell that consumer's Personal Data;

(4) **Consumer Opt-In for Minors** - Conversely, consumers who are minors (under thirteen) can opt-in to the sale of their Personal Data with the affirmative consent of their parent or guardian, and minors (aged 13-16) can opt-in with their affirmative consent; and

(5) **Non-Discrimination for Exercise of Consumer Rights** – Covered Businesses cannot discriminate against consumers who exercised their rights pursuant to the CCPA by: (a) refusing to sell that consumer goods or services, (b) charging different prices to that consumer unless such price difference is "reasonably related" to the value of the Personal Data, or (c) provide lower quality goods or services to that consumer.[165]

Failure to comply with the CCPA subjects the violating company to civil penalties of up to

---

[162] CAL. CIV. CODE § 1798.100 et seq. (West 2018).

[163] An introductory statement to the bill that would eventually become the CCPA stated: "In March 2018, it came to light that tens of millions of people had their personal data misused by a data mining firm called Cambridge Analytica. A series of congressional hearings highlighted that our personal information may be vulnerable to misuse when shared on the Internet. As a result, our desire for privacy controls and transparency in data practices is heightened." Assemb. B. 375 § 2(g), 2017-2018 Leg., Reg. Sess. (Cal. 2018).

[164] Assemb. B. 375, 2017-2018 Leg., Reg. Sess. (Cal. 2018).

[165] John Stephens, *California Consumer Privacy Act*, ABA BUS. AND CORP. COMMITTEE NEWSL. (Feb. 14, 2019), https://www.americanbar.org/groups/business_law/publications/committee_newsletters/bcl/2019/201902/fa_9/.

$7,500 per violation[166] or permits consumers to bring a class action and obtain statutory damages of $100-$750 per incident. The violating company has thirty days to cure and must provide the consumer with a written statement that the violation is cured.[167] The CCPA was subsequently updated to, among other things: (1) clarify that data identifiers are only considered to be Personal Data if those identifiers can be connected to an individual or household; (2) avoid conflict with other regulations; and (3) commence enforcement "six months after the publication of final regulations issued pursuant to this section or July 1, 2020, whichever is sooner."[168]

It is estimated that companies will spend as much as $55 billion to comply with the CCPA, ranging from $467 million to $16 billion just in the next decade.[169] Price Waterhouse Coopers ("PWC") estimates that a fifth of large companies will spend $100 million and add over fifty employees to comply, and that 28% of those companies expect revenue impact due to CCPA.[170] An additional clear impact from the CCPA is companies' addition of technological resources to assist with compliance, which represents a significant change from when companies geared up to comply with GDPR. To comply with GDPR, PWC determined that most companies created manual, labor-intensive processes and capabilities. Based on the learnings from GDPR compliance, companies plan to rely more on technology, despite the high expenditures to do so, in order to, among other things, handle the high volume of expected consumer calls.[171] These kind of large expenditures made by companies to comply with the CCPA demonstrate that the CCPA is another regulatory disruptor.

As of this writing one case is pending under the CCPA, *In re Hanna Andersson and Salesforce.com Data Breach Litigation*.[172] In the Hanna Andersson case, class action plaintiffs allege a data breach occurred due to malware infecting Hanna Andersson's e-commerce platform operated by Salesforce.com. However, the data breach referenced occurred before the CCPA went into effect and thus the case is likely to be dismissed, but the case does surface some interesting issues, namely that: (1) the CCPA does not permit retroactive application; (2) unlike the GDPR, the CCPA does not require a company to maintain reasonable security measures but does allow consumers to pursue statutory damages in the event of a data breach; (3) unlike the GDPR, the CCPA gives companies a right to cure before penalties are imposed; (4) unlike the GDPR, the CCPA does not hold "service providers", an entity processing Personal Data on behalf of a business pursuant to a written contract, liable for data breaches; (5) unlike the GDPR, the CCPA only requires businesses that own, license or maintain Personal Data to maintain

---

[166] CAL. CIV. CODE §§ 1798.150(a)(1)(A), 1798.155(b) (West 2018).

[167] CAL CIV. CODE §1798.150(b).

[168] Stephens, *supra* note 165 (citing 2018 Cal. ALS 735; 2018 Cal. SB 1121; 2018 CAL. STATS. ch. 735; 2018 Cal. ALS 735; 2018 Cal. SB 1121; 2018 CAL. STATS. ch. 735, § 1798.185(a)).

[169] Lauren Feiner, *California's new privacy law could cost companies a total of $55 billion to get in compliance*, CNBC.COM (Oct. 5, 2019), https://www.cnbc.com/2019/10/05/california-consumer-privacy-act-ccpa-could-cost-companies-55-billion.html.

[170] *Survey: One-fifth of large companies will spend over $100 million, add over 50 staff on CCPA*, PRICE WATERHOUSE COOPERS (June 13, 2020), https://www.pwc.com/us/en/services/consulting/cybersecurity/california-consumer-privacy-act/pulse-survey-large-companies-spend-over-100-million.html.

[171] Two-thirds of the companies surveyed by PWC expect over 500 consumer calls per day, and 11% of the companies surveyed expect over 10,000 calls per day. *Id.*

[172] No. 3:20-cv-00812-EMC (N.D. Cal. filed Feb. 3, 2020).

reasonable security procedures.[173]

The CCPA is not the only law that addresses the privacy of biometric data; however, the CCPA's definition of biometric data is actually more broad than the Illinois Biometric Information Privacy Act ("BIPA"),[174] the first and oldest biometric regulation in the United States,[175] because the CCPA includes information from which an "identifier template" can be created, such as such as "imagery" of an individual's palm or vein patterns, voice recordings, and "keystroke patterns or rhythms". There is currently a class action pending[176] regarding the privacy of biometric data under BIPA. In that case, the plaintiffs allege that White Castle failed to get adequate consent before collecting fingerprint data, and that White Castle wrongly provided the fingerprint data to third party vendors without permission. Illinois passed the BIPA in 2008 in response to the risk of identity theft. The BIPA defines a "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." The law specifically states that the individual's biometric data cannot be disclosed, redisclosed or disseminated without the individual's permission, and further that no private entity can "sell, lease, trade, or otherwise profit" from an individual's biometric information.[177] White Castle moved for judgment on the pleadings, alleging that plaintiffs' claims were barred by the statute of limitations because more than five years had lapsed since White Castle originally collected plaintiff's biometric data, but the court denied defendants' motion, holding that it was "inconceivable" that the Illinois legislature intended for claims under the BIPA to accrue only at the time of initial collection of the biometric data when "it is readily apparent that entities can continuously and repeatedly engage in the kind of conduct BIPA is designed to deter."[178]

Cothron joins a long list of cases regarding the privacy of biometric data, most of which targeted employers; however, Facebook is also in the midst of fighting a class action for violation of the BIPA due to Facebook's use of facial recognition technology to enable its users to recognize their Facebook friends from uploaded photos.[179] Facebook is facing billions in potential fines for breach of BIPA. Although the biometric data technology is enticing, the possible theft of biometric data is viewed as a much higher risk because there is little recourse if your biometric data is stolen. Shawn Williams, the attorney for the plaintiffs in the Facebook case, said "It's not like a Social Security card or credit card number where you can change the number. You can't change

---

[173] Ron Raether et al., *INSIGHT: First CCPA-Related Case Foreshadows Five Issues*, BLOOMBERG LAW (Feb. 10, 2020), https://news.bloomberglaw.com/privacy-and-data-security/insight-first-ccpa-related-case-foreshadows-five-issues-5.

[174] 740 ILL. COMP. STAT. 14/1-99 (enacted in October of 2008).

[175] Other states having biometric laws are Texas, Washington, New York and Arkansas. For information regarding those laws, *see* Natalie A. Prescott, *The Anatomy of Biometric Laws: What U.S. Companies Need to Know in 2020*, NATIONAL LAW REVIEW (Jan. 15, 2020), https://www.natlawreview.com/article/anatomy-biometric-laws-what-us-companies-need-to-know2020#:~:text=While%20BIPA%20remains%20the%20only,laws%20to%20include%20biometric%20identifiers.

[176] *See* Cothron v. White Castle Sys., Inc., No. 19 CV 00382, 2020 WL 3250706, at *2 (N.D. Ill. June 16, 2020).

[177] 740 ILL. COMP. STAT. 14/15(c).

[178] *Cothron*, 2020 WL 3250706, at *14.

[179] In re Facebook Biometric Info. Privacy Litig., 326 F.R.D. 535 (N.D. Cal. 2018), *aff'd sub nom*. Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019), *cert. denied*, 140 S. Ct. 937, 205 L. Ed. 2d 524 (2020).

your face."[180]

Facebook's experience in the Facebook class action described previously may have precipitated its latest move - Limited Data Use. Effective July 1, 2020, Facebook implemented a new feature called "Limited Data Use" or "LDU", to require advertisers to comply with Facebook's "State-Specific Terms"[181], which limit the way user data can be stored and processed in Facebook for any user that Facebook identifies as a California resident.[182] Facebook will automatically default to LDU until July 31, 2020, at which time businesses must update their pixel to include a LDU parameter.[183] Facebook's LDU enables advertisers to specify if users' data should be subject to CCPA and transfers liability for compliance with the CCPA to the advertiser. Google also has a similar feature for restricted data processing for its services Ad Manager, Ad Manager 360, AdMob, or AdSense. Under Google's restricted data processing, Google will restrict how it uses certain unique identifiers and other data processed in the provision of services. Google will not create or update profiles for ads personalization, use existing profiles to serve personalized ads relating to data to which restricted data processing applies, or serve programmatic ads that utilize third-party ad tracking or third-party ad serving and bid requests will not be sent to third-party programmatic buyers.[184] Franchisors now face the disruption from Facebook and Google requiring franchisors to obtain the services of a developer to change their Facebook pixel or to adjust the franchisors' personalized or programmatic advertising.

3. Other State Privacy Laws Giving Opt-Out Rights[185]

Nevada enacted the Privacy of Information Collected on the Internet from Consumers Act effective October 1, 2019[186] granting consumers the right to opt-out of the sale of their PII effective no later than 60 days after sending a "verified request" to the covered "operator". A verified request, under this law, is a request that the covered "operator" can "reasonably verify the authenticity of the request and the identity of the consumer using commercially reasonable means".[187] Although similar to the CCPA, Nevada's law defines sales more narrowly as the sale

---

[180] Jonathan Stempel, *Facebook loses facial recognition appeal, must face privacy class action*, REUTERS TECHNOLOGY NEWS (Aug. 8, 2019), https://www.reuters.com/article/us-facebook-privacy-lawsuit/facebook-loses-facial-recognition-appeal-must-face-privacy-class-action-idUSKCN1UY2BZ.

[181] State-Specific Terms, FACEBOOK, Effective July 1, 2020, https://www.facebook.com/legal/terms/state-specific/update.

[182] Data Processing Options for Users in California, FACEBOOK FOR DEVELOPERS, https://developers.facebook.com /docs/marketing-apis/data-processing-options/ (last visited Aug. 31, 2020).

[183] Developers will need to include a string within the Facebook pixel for "dataProcessingOptions" to specify your degree of CCPA compliance. Simon Poulton, *Facebook CCPA compliance challenges: Limited Data Use*, SEARCH ENGINE LAND (July 2, 2020), https://searchengineland.com/facebook-ccpa-compliance-challenges-limited-data-use-337170/.

[184] *Helping advertisers, publishers, and partners comply with the California Consumer Privacy Act (CCPA)*, GOOGLE (July 21, 2020), https://privacy.google.com/businesses/rdp/.

[185] For an overview of state internet privacy laws, *see State Laws Related to Internet Privacy*, NAT'L CONFERENCE OF STATE LEGISLATURES (Jan. 27, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx/.

[186] NEV. REV. STAT. ANN. § 603A.300-603A.360.

[187] *Id.* at § 603A.337.2.

of PII for "monetary consideration"[188], unlike the CCPA, which includes the sale of PII for "other valuable consideration."[189] The Nevada law also exempts covered "operators" such as financial institutions covered by the Gramm-Leach-Billey Act, health care providers subject to HIPAA, manufacturers and servicers of motor vehicles, and third parties that support the covered operator's business.[190] Penalties include injunctive relief or up to $5,000 per violation, enforceable by the State Attorney General's Office.[191]

Vermont also gives consumers the right to opt-out of the sale of the consumer's data by requiring data brokers (businesses that knowingly collect and license PII of consumers with whom the data broker does not have a direct relationship), to provide consumers with a notice of whether the consumer may opt-out of the collection and sale of their PII.[192] Vermont also requires the data broker to disclose to the consumer: (1) the name, email and internet addresses of the data broker; (2) whether the consumer can authorize a third party to provide an opt-out on the consumer's behalf; (3) the data collection, databases and/or sales activities that are not available for opt-out; and (4) if the data controller has a purchaser credentialing process.

Maine just enacted the "Act to Protect the Privacy of Online Customer Information" that took effect on July 1, 2020 (the "Maine Privacy Act").[193] The Maine Privacy Act prohibits providers of broadband internet service from using, disclosing, selling or permitting access to a customer's personal information unless the customer expressly consents to that use, disclosure, sale or access. The Maine Privacy Act also protects other information that the broadband service may collect about the user that is not personal information if the customer opts-out.[194]

4. <u>Additional state legislation/regulations to come</u>

The constantly shifting and evolving technological landscape will cause additional legislation and regulations to come to bear, especially as hackers continue to obtain, use, and sell private information. The latest proposed legislation shows concern in the areas of social media and PCI.

Most recently, on March 12, 2020, Senator Jerry Moran of Kansas introduced the Consumer Data and Privacy Act of 2020, which proposed a federal framework for consumer data

---

[188] *Id.* at § 603A.333.1.

[189] Foley & Lardner, LLP, The Nevada Privacy Law Is No CCPA, but Beware of Noncompliance, October 3, 2019, https://www.jdsupra.com/legalnews/the-nevada-privacy-law-is-no-ccpa-but-50773/.

[190] NEV. REV. STAT. ANN. § 603A.330.2.

[191] *Id.* at § 603A.360.

[192] VT. STAT. ANN. tit. 9, § 2446.

[193] ME. STAT. tit. 35-A, § 9301.

[194] Under the Maine Privacy Act, the type of geofencing discussed earlier in this paper is impermissible unless the customer specifically consents. Several trade associations whose members include Internet Service Providers ("ISPs") in the State of Maine sought declaratory and injunctive relief from the Maine Privacy Act, alleging that it was unconstitutional and preempted by federal law. The ISPs moved for judgment on the pleadings and that motion was denied. *See* ACA Connects - Am.'s Commc'ns Ass'n v. Frey, No. 1:20-CV-00055-LEW, 2020 WL 3799767 (D. Me. July 7, 2020).

privacy that would preempt prior state laws on the subject.[195]The bill would prohibit the collection or processing of personal data by any business without the express or implied consent of the consumer, unless the collection or processing is necessary to provide a service or perform under an existing contract with the consumer.[196] The Federal Trade Commission would be entitled to enforce these laws by imposing a civil penalty equal to the number of individuals affected by any violation multiplied by a maximum penalty of $42,530.[197] Additionally, state attorneys general would have a right to bring a civil action under the law.[198] The law, however, would not provide a private right of action to consumers,[199] a significant change from the CCPA, which would be preempted by this new federal law. As of this publication's date, no further action has been taken on this bill.

In a similar vein, the Ensuring National Constitutional Rights for Your Private Telecommunications Act of 2019 (the "Encrypt Act") is federal legislation proposed by Congressman Ted W. Lieu of California, Congresswoman Suzan DelBene of Washington and Congressman Jim Jordan of Ohio on August 6, 2019.[200] The Encrypt Act, if enacted, would prohibit states and localities from establishing their own encryption standards for software or technology and from requiring the makers of such software or technology to decrypt their software or technology for surveillance purposes, leaving the technology vulnerable to attacks.[201] In his introduction of the bill, Congressman Lieu stated that allowing state and local governments to require technology developers to meet different mandatory encryption standards with different levels of security, would leave customer data open to threats from hackers, and proposes instead a federal standard to better protect that data.[202] Congresswoman DelBene stated:

> Keeping people's information secure must be a priority for Congress. Without a national encryption policy, we cannot effectively protect personal data, leaving individuals susceptible to attacks from bad actors. This legislation unifies our encryption methods to provide security to the American people while ensuring that advances in technology can continue to grow.[203]

As of September 25, 2019, the Encrypt Act was referred to the Subcommittee on Crime,

---

[195] Consumer Data Privacy and Security Act of 2020, S. 3456, 116th Cong. § 10(b) (2020) (describing preemptive effect of the law, but accepting laws relating to notification following data breaches and other general statutory schemes relating to tortious actions, such as fraud).

[196] *Id.* at § 3(a)-(c).

[197] *Id.* at § 9(a).

[198] *Id.* at § 9(b).

[199] *Id.* at § 9(d).

[200] Ensuring National Constitutional Rights for Your Private Telecommunications Act of 2019, H.R. 4170, 116th Cong. (2019).

[201] *Id.*

[202] *Rep. Lieu Announces Encrypt Act Reintroduction at Defcon*, TED LIEU (Aug. 9, 2019), https://lieu.house.gov/media-center/press-releases/rep-lieu-announces-encrypt-act-reintroduction-defcon.

[203] *Id.*

Terrorism, and Homeland Security, where it still awaits a hearing.[204]

And in yet another effort to create more security at the federal level, the Eliminating Abusive and Rampant Neglect of Internet Technologies Act of 2019 (the "Earn IT Act") [205] was introduced on March 5, 2020 by Senators Lindsey Graham of South Carolina, Richard Blumenthal of Connecticut, Josh Hawley of Missouri, and Dianne Feinstein California. The bill would require internet companies to "earn" protection from liability for illegal content posted by users, and in particular images of child abuse and sex trafficking. It is not yet known whether the Earn IT Act will enable law enforcement access to content; however, Senator Graham stated: "Facebook is talking about end-to-end encryption which means they go blind…We're not going to go blind and let this abuse go forward in the name of any other freedom."[206] On July 2, 2020, the EARN IT Act was ordered to be reported out of the Senate Committee on the Judiciary to the full Senate for full review with the support of the majority of the committee. This is yet another bill to watch, as it could mean franchisors could be held liable for illegal content posted by franchisees on the brand's intranet, for example.

In the coming years, we should expect to see additional privacy law developments both domestically and around the globe. Florida introduced a privacy bill in 2019, however, the bill died in committee on March 24, 2020.[207] New Hampshire also introduced a privacy bill in 2019 and it is now under further consideration.[208] Washington similarly has a privacy bill proposed in the legislature, but it has twice failed to be passed by the legislature, most recently failing when the state senate refused to accept amendments made by the state house.[209] These bills are all similar to the CCPA, but in some ways are more restrictive. New Hampshire's bill, for example, does not require that the PII collected be "reasonably capable" of being associated with an individual, covers PII that is nonencrypted or nonredacted, and is not limited to online or digital PII collection.[210]

C. <u>Data Collection and Ownership</u>

In this era of Big Data and especially with the complex web of third parties providing pieces and parts of technology used by franchisors, such as online ordering and POS, it is increasingly difficult to determine who owns, or is responsible for, the data generated by or obtained from the

---

[204] H.R. 4170, 116th Cong. (2019) (full text available at https://www.congress.gov/bill/116th-congress/house-bill/4170?s=1&r=1).

[205] EARN IT Act of 2020, S. 3398, 116th Cong. (2020), (full text available at https://www.congress.gov/bill/116th-congress/senate-bill/3398/text).

[206] Casey Newton, *A sneaky attempt to end encryption is worming its way through Congress*, THE VERGE (Mar. 12, 2020), https://www.theverge.com/interface/2020/3/12/21174815/earn-it-act-encryption-killer-lindsay-graham-match-group.

[207] *HB 963: Consumer Data Privacy*, THE FLORIDA SENATE, https://www.flsenate.gov/Session/Bill/2020/963/.

[208] The New Hampshire bill was referred for interim study on March 11, 2020. *HB1680*, GENERAL COURT OF NEW HAMPSHIRE – BILL STATUS SYSTEM, http://gencourt.state.nh.us/bill_status/bill_status.aspx?lsr=2535&sy=2020&txtsessionyear=2020&txtbillnumber=hb1680&sortoption=&q=1.

[209] Byron Mühlberg, *Washington Privacy Act Fails to Pass, Again*, CPO MAGAZINE (Apr. 6, 2020), https://www.cpomagazine.com/data-protection/washington-privacy-act-fails-to-pass-again/.

[210] H.R. 1680, 2019-2020 Leg., Reg. Sess. (N.H. 2019).

technology. As explained earlier in the article, data may be obtained by one source but is then passed to another party to use the data or perform a different task. For example, farmers can use smart tractors that utilize GPS to plant corn and determine where the farmer gets the best yields. Monsanto asked farmers for their data so that Monsanto could analyze it to give farmers information on how best to work their fields to obtain higher yields and more profits.[211] Who owns the data now – Monsanto or the farmer? More importantly, does it matter who owns the data?

One reason a company may prefer to own data is to enable that company to exclusively market to its customers. However, based on today's technology and legal framework, one can argue that rights to use Big Data and liability for Big Data are more critical than ownership of the data. For that reason, if a company supplies its data to a third party for analysis or to perform some other function, the contract with that third party should include provisions regarding how the data can be used and liability for misuse of the data. In light of the rapidly changing legislative landscape, franchise systems need to include provisions in contracts with vendors that access, use, or process their data in order to protect against exposure for any security breaches. These provisions should clearly specify which party controls the data, how the data will be used, if the data can be sold, where the data will be stored, whether the data can be shared with any third party, and which party is responsible for maintaining security features. Further, processes and procedures need to be in place to respond to consumer requests to delete any data, as well as to respond to any data breach that may occur.[212] Recall that the CCPA requires only a party that owns, licenses, or maintains Personal Data to have reasonable security procedures for that information, and thus, if the franchisor or franchisee are using software-as-a-service solutions, which do not maintain or store data, the contract should clarify which party has the obligation to maintain security of the Personal Data.[213]

Franchise systems should also consider updating their insurance requirements for vendors who access, use, or process a franchise system's data, especially any PII, to include coverage for data breaches and violations of data privacy laws. Franchise systems should also require vendors to indemnify the franchisor and franchisees for any damages arising from a data breach or violations of data privacy laws. Adding these items to vendor contracts not only helps to ensure a proper understanding of expectations related to data privacy and protection, but also properly allocates the risk of any loss caused by a vendor's failure.

D. <u>Data Breach Responses</u>

A data breach response plan is a set of specific, planned, and coordinated steps an organization takes to identify and respond to data breaches quickly. The plan includes technology such as anti-malware software and data encryption, as well as policies and processes. The GDPR requires companies to respond to a data breach within seventy-two hours, so having a good data breach response plan is critical; however, Price Waterhouse Coopers estimated, in 2018, that only 30% of companies have such a plan in place.[214] A data breach response plan should require the company to: (1) have procedures to spot a breach quickly; (2) establish investigation and

---

[211] Daniel Burrus, *Who Owns Your Data?*, WIRED (Feb. 2014), https://www.wired.com/insights/2014/02/owns-data/.

[212] Raether, *supra* note 173.

[213] *Id.*

[214] Julia Dutton, *Do you have a data breach response plan?*, IT GOVERNANCE (Mar. 12, 2019), https://www.itgovernance.co.uk/blog/do-you-have-a-data-breach-response-plan.

clean-up parameters for breach incidents – what notices need to be sent, when the system can be used again, etc.; (3) determine what happened; (4) determine what was compromised – systems, networks and data; (5) determine if the data was stolen, deleted or corrupted; (6) find out who or what caused the breach and why using forensics; (7) analyze the incident and ways to prevent it in future; and (8) determine the business impact.[215]

So how do data breaches happen? The top six reasons are: (1) physical actions; (2) misuse of privileges; (3) social engineering; (4) human error; (5) malware; and (6) hacking.[216] Physical actions include the theft of laptops, phones, storage devices, paperwork and card skimming, where a device card is inserted into a card reader or ATM to obtain PCI. These physical actions can be thwarted by maintaining control over devices and passwords. The misuse of privileges category covers employees who use information improperly by copying, sharing, accessing, or stealing. Social engineering is another broad category that covers phishing (targeting individuals under false pretenses to acquire their information) and financial pretexting (phishing to get financial information by phone, email or duplicating legitimate websites). Malware, probably the most well-known cause of data breach, is any type of malicious software designed to harm or exploit any programmable device, service, or network. Email is still responsible for the majority of malware infecting a system.[217] Attackers are now exploiting MS Office to disguise malware in Word documents to convince users that the document is legitimate.[218] It is estimated that the total cost of malware will exceed $6 trillion by 2021.[219] For purposes of this paper, malware also includes ransomware, a form of malware that encrypts a victim's files, enabling the attacker to demand something to restore the victim's access.[220] Although ransomware may be on the decline, it is estimated this year alone that victims will pay $11.5 billion to attackers,[221] and local governments appear to be the favorite target.[222] The last, and most prevalent, reason that data breaches occur is hacking.[223] Just in January 2019 alone, an estimated two billion records were hacked, including records from 202 million Chinese citizens and an FBI investigations

---

[215] Julia Dutton suggests the following guides to create a data breach response plan: (1) *10 Steps to Cyber Security*, NATIONAL CYBER SECURITY CENTRE (Jan. 19, 2019), https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/introduction-to-cyber-security/executive-summary; or (2) the EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY, GOOD PRACTICE GUIDE FOR INCIDENT MANAGEMENT (2010). Dutton, *supra* note 214.

[216] Luke Irwin, *The 6 most common ways data breaches occur*, IT GOVERNANCE (Mar. 12, 2019), https://www.itgovernance.eu/blog/en/the-6-most-common-ways-data-breaches-occur.

[217] Out of 50,000 incidents, email represented 92% of the malware installation attempts. Andrew Sanders, *15 (Crazy) Malware and Virus Statistics, Trends & Facts 2020*, SAFETY DETECTIVES (Jan. 30, 2020), https://www.safetydetectives.com/blog/malware-statistics/.

[218] Sanders estimates 38% of malware is now disguised as a Word document. *Id.*

[219] In 2015, the estimated cost of malware was $500 billion and by 2020 it topped $2 trillion. *Id.*

[220] Josh Fruhlinger, *Ransomware explained: How it works and how to remove it*, CSO (Dec. 19, 2020), https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html.

[221] Sanders, *supra* note 217.

[222] Dan Lohrman, *2019: The Year Ransomware Targeted State & Local Governments*, GOVERNMENT TECHNOLOGY (Dec. 23, 2019), https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2019-the-year-ransomware-targeted-state--local-governments.html.

[223] Irwin estimates as many as 48% of data breaches are due to hacking. Irwin, *supra* note 216.

database.[224] Why should franchisors be concerned? Attackers target small businesses (businesses having fewer than 1,000 employees) that do not have the manpower or financial resources to defend attacks.[225] The majority of small businesses that suffer cyberattacks are out of business within six months.[226]

Based on the prevalence and risk to the franchisee, should a franchisor provide data privacy assistance to its franchisees? Encouraging franchisees to have a data breach response plan, especially one that notifies the franchisor is important, not only because of potential harm to the brand, but also because of the possible liability the franchisor may face depending on the reason for the data breach. The franchisor also risks reputational harm if it does not at least suggest a planned public relations/media response to franchisees to address the data breach and reduce any public perception that the breach is attributable to the franchisor. Franchisors should also encourage their franchisees to have cyber insurance coverage to help franchisees fund costs incurred due to the data breach, including notification, restoring personal identities, recovering data, and repairing any damaged systems.[227] The amount of coverage will vary depending upon the sensitivity and amount of Personal Data franchisees have or use or allow others to have or use.

Payment Card Information, or "PCI", is an example of sensitive Personal Data. The rise of payment cards as a method of payment has been meteoric, starting with the first bank-issued charge card in 1946 and the creation of "chip" cards in 1994, causing businesses to upgrade their POS to process chip card transactions. In 2015, debit card use surpassed all other forms of non-cash payments, such as checks and credit cards, and 46% of American consumers preferred to use debit cards as a form of payment. Nowadays, accepting mobile payments where a card is not present are becoming de rigueur. Those payments are made via a debit card, credit card, or smartcard enabled with RFID or near-field communication ("NFC") technology that enables two devices to communicate with each other and exchange data.[228]

In the late 1990s, the credit industry was besieged by credit card fraud, phishing, hacking, and other web-based schemes. After credit card fraud losses reached $750 million per year, the industry was forced to adopt measures to decrease the fraud. Five major credit card companies, Visa, MasterCard, American Express, Discover, and JCB created the Payment Card Industry Data Security Standard (the "PCI-DSS") 1.0 in December 2004 to close loopholes exploited by hackers, phishers, and fraudsters. The PCI-DSS is not a law, but are security standards[229]

---

[224] Sanders, *supra* note 217.

[225] Sanders estimates 61% of data breach victims in 2017 had fewer than 1,000 employees. Only 14% of small businesses believe their ability to fend off cyberattacks is highly effective, and a whopping 51% of small businesses are not allocating any budget to implement measures to decrease cyberattacks. *Id*.

[226] *Id.*

[227] *What is Cyber Insurance?*, NATIONWIDE SMALL BUSINESS RESOURCES (June 14, 2020), https://www.nationwide.com/lc/resources/small-business/articles/what-is-cyberinsurance#:~:text=Cyber%20insurance%20generally%20covers%20your,license%20numbers%20and%20health%20records.

[228] *Payment Methods: A Brief History and a Look to the Future*, CARDKNOX (June 13, 2020), https://www.cardknox.com/white-papers/payment-methods-history-and-future/.

[229] These standards are: (1) PCI-PED – manufacturers that require personal identification numbers at payment terminals; (2) PCI PA-DSS – software developers and integrators that store, process or transmit cardholder data as part of authorization of settlement, including applications sold, distributed or licensed to third parties; and (3) PCI-DSS

adopted and administrated by the Payment Card Industry Security Standards Council (the "PCI SSC"), and it is applied to any organization, regardless of size, that accepts, transmits, or stores any cardholder data, including through a payment application. The level of compliance an organization must meet is determined by Visa transaction volume over a twelve-month period. If an organization fails to comply, the payment brands may fine the acquiring bank $5,000 to $100,000 per month, and the acquiring bank generally passes these fines to the merchant. Compliance is determined through a self-assessment questionnaire (SAQ) and, depending upon the compliance level the organization must meet, through a passing score on a vulnerability scan administered by a PCI SSC Approved Scanning Vendor (ASV) that is submitted to the acquiring bank.[230] For franchise systems that accept credit cards as a method of payment from the consumer or their franchisees, the PCI-DSS applies.

Franchisors must weigh the possible adverse effect on their brand and reputational harm in the event of a data breach involving PCI versus the risk of vicarious liability resulting from franchisor-imposed controls. The two oft-cited cases involving franchisors, franchisees, and PCI data breaches are *FTC v. Wyndham Worldwide Corp*.[231] and *In the Matter of Aaron's*.[232] In *Wyndham*, the FTC sought to hold Wyndham, as franchisor, liable for three data breaches of the property management system Wyndham required its franchisees to use.[233] The FTC alleged the breaches caused Wyndham customers to suffer from fraudulent charges on their accounts and also cause the release of hundreds of thousands of credit card numbers to an internet domain address registered in Russia. The FTC also asked the court to hold Wyndham vicariously liable for the breaches even though the customer information was obtained from customers by Wyndham's franchisees. Ultimately the FTC and Wyndham reached a settlement in which the FTC agreed that Wyndham, as a franchisor, was not liable for the actions or failures of its franchisees resulting in the data breach, but the settlement did require Wyndham to maintain a security program for twenty years, identify data breach risks at Wyndham hotels, implement reasonable safeguards to control data breach risks, and certify whether any Wyndham network was an untrusted network.[234]

In *Aaron's*, the FTC alleged that Aaron's, the franchisor, "knowingly assisted" its franchisees in violating privacy laws by allowing them to access Aaron's required third-party software and activate "cyber-spying software."[235] That software enabled franchisees to monitor customers' keystrokes and use web-cameras on the computers the franchisees rented to consumers and permitted franchisees to transmit and store the emails the franchisee's obtained

---

– any entity that stores, processes and/or transmits cardholder data. *At a Glance: Standards Overview*, PCI SECURITY STANDARDS COUNCIL (June 2008), https://www.pcisecuritystandards.org/pdfs/pcissc_overview.pdf.

[230] *PCI FAQs*, PCICOMPLIANCEGUIDE.ORG, https://www.pcicomplianceguide.org/faq/.

[231] 799 F.3d 236 (3rd Cir. 2015).

[232] No. 122-3264, 2014 WL 1100702 (F.T.C. Mar. 10, 2014).

[233] Wyndham's property management system processed Personal Data and PCI that included payment card account numbers, expiration dates, and security codes. *Wyndham*, 799 F.3d at 240.

[234] Luehr, *supra* note 148.

[235] *Aaron's*, 2020 WL 1100702, at *1.

from the cyber-spying software.[236] Aaron's also provided the franchisees technical support for the software, including information about how to install the program in a way to avoid anti-virus software.[237] Aaron's did not suggest its franchisees use the cyber-spying software, nor did Aaron's use the cyber-spying software in its company locations.[238] Aaron's ultimately agreed to a consent order with the FTC, by which it was enjoined from using any monitoring technology to gather information about consumers who rented computers or received data from such rented computers and was required to stop all deceptive practices related to consumer data collection.[239] Aaron's was permitted, however, to gather data or information from any consumer product based on "geophysical location tracking technology" provided the consumer received a prominent notice at the time of rental and the consumer gave affirmative express consent to such tracking.[240] Further, Aaron's was required to modify its franchise agreements or otherwise prohibit its franchisees from any conduct barred by the consent order and required to annually review its franchisees' compliance with the order.[241] Finally, Aaron's was required to ensure that franchisees who violate the order stop their conduct and to terminate franchisees who continue to violate the order.[242]

What then, is the main difference between *Wyndham* and *Aaron's*? In *Aaron's*, the franchisor provided franchisees with assistance that enabled them to violate data privacy laws and PCI-DSS. Before providing any advice, tools or training to its franchisees, franchisors should first ensure that doing so will not be deemed knowing assistance that helps a franchisee to violate privacy laws and/or PCI-DSS.

E. <u>Changes to the Franchise Agreement</u>

Because of the evolution of technology, franchisors should plan to update provisions in their franchise agreements and any other contracts with their franchisees that are needed to

---

[236] *Id.*

[237] *Id.* at *2.

[238] *Id.* at *3.

[239] *Id.* at *6-10.

[240] Specifically, Aaron's was required to provide the following: "Clear and Prominent Notice: respondent shall provide a clear and prominent notice to the user, separate and apart from any "privacy policy," "data use policy," "terms of service," "end-user license agreement," "lease agreement," or other similar document, that discloses (1) that geophysical location tracking technology is installed and/or currently running on the rented consumer product; (2) the types of user activity or conduct that is being captured by such technology; (3) the identities or specific categories of entities with whom any data or information that is collected will be shared or otherwise provided; (4) the purpose(s) for the collection, use, or sharing of such data or information; and (5) where and how the consumer can contact someone for additional information; and 2. Affirmative Express Consent: respondent shall obtain affirmative express consent by giving the renter an equally clear and prominent choice to either agree or not agree to any geophysical location tracking technology, and neither option may be highlighted or preselected as a default setting. Activation of any geophysical location tracking technology must not proceed until the renter provides affirmative express consent. Notwithstanding the foregoing, nothing in this Section shall require respondent to rent an item to a consumer who declines to consent to installation or activation of any geophysical tracking technology…." Agreement Containing Consent Order, *In the Matter of Aarons*, No. 122-3264, 2014 WL 1100702 (F.T.C. Oct. 22, 2014) (available at https://www.ftc.gov/sites/default/files/documents/cases/131022aaronsagree.pdf).

[241] *Aaron's*, 2020 WL 1100702, at *9-10.

[242] *Id.*

license software or use data. Some suggested changes are: (1) require franchisees, and any third parties receiving Personal Data from the franchisee, to adhere to privacy laws regarding Personal Data; (2) require franchisees to adopt and enforce data security procedures and develop a data breach response plan; and (3) require franchisees to obtain cyber insurance commensurate with the sensitivity and amount of Personal Data they have or use. In addition to including these contractual requirements, franchisors should consider how to monitor compliance and what actions to take if a franchisee does not comply, such as obtaining cyber insurance on the franchisee's behalf (presumably charged back to the franchisee) or requiring the franchisee to engage a data security consultant. Franchisors should, however, evaluate all contractual provisions, requirements, monitoring and assistance through a *Wyndham/Aaron's* lens to avoid becoming too involved in the franchisee's operations and thus creating vicarious liability for the franchisor. [243]

IV. FOODBORNE ILLNESS IN A FRANCHISE SYSTEM

Little can stop a restaurant in its tracks faster than a foodborne illness. Between recalls, closures, customer illnesses, and even possible deaths, an outbreak can have a severe and long-lasting impact on a brand and the public's association of illness with that brand. In a franchise system, the stakes can be even higher where identifying and arresting the source of the outbreak is challenged by the franchisor's lack of operational control over the individual restaurants. The source of an outbreak may be at a supplier level or the result of a poorly operating franchisee, either of which will impact the franchisor's notice and response plan. In more fortunate circumstances, a supplier may notify the franchisor of a food safety threat before any customers become ill. In less fortunate circumstances, franchisors discover the contamination only after customers begin suffering severe illnesses or even deaths.[244] Regardless of the cause of the contamination, franchisors and franchisees must work together quickly to identify the contamination source and contain the spread of the disease. And while public health is always the top priority, restaurants will also want to be sure their actions do not compromise consumer confidence, insurance coverage, or their legal claims and defenses. This section will discuss a franchise system's liability in foodborne illness outbreaks, how franchise systems navigate the legal minefield ahead, and some of the preventative actions a franchisor can take to stop an outbreak before it starts – or lessen the blow after it does.

A. Legal Exposure within a Franchise System

1. Franchisor and Franchisee liability to consumers

The scope of a franchisor's and its franchisees' liability for a foodborne illness outbreak

[243] David Ramsey aptly states that "there is a balance the franchisor must strike: provide the franchisee with advice, guidance, and assistance (and even requirements where needed to protect the brand), but do not become too involved in franchisee operations to the point of risking vicarious liability claims against the franchisor." David B. Ramsey, *CYBER CENTER: Cyber-Security Considerations for Franchisors: Protecting the Brand While Avoiding Vicarious Liability*, ABA BUSINESS LAW TODAY (July 20, 2016), https://www.americanbar.org/groups/business_law/publications/blt/2016/07/cyber_center/.

[244] Identifying the source of the outbreak can be complicated. *See, e.g.,* William D. Marler and David W. Babcock, *How to Document A Food-Poisoning Case: Your Client Got Salmonella Poisoning After Eating Breakfast at A Restaurant Weeks Ago. The Food Is Long Gone - Eaten or Thrown Out. With the Right Documents, You Still Have A Case*, TRIAL, Nov. 2004, at 36 (describing an instance where although there had been a supplier-sourced e-coli outbreak in the hamburger meat used in a restaurant, the restaurant's meat was not contaminated and the source of the e-coli injuring a consumer was from poor-handling methods).

will depend largely on both the facts of the case and the jurisdiction where the outbreak takes place. As a result, in the case of a nationwide or multi-state outbreak, a franchisor may be navigating a complex web of state laws to determine the full scope of its liabilities and responsibilities upon an outbreak. The very first thing to determine whenever there is an outbreak is the source. If the source of the outbreak is from an operator's poor handling of the product, then the operator or franchisee will be primarily liable for the failures; however, a franchisor may still face vicarious liability claims. If, on the other hand, the outbreak is at the supplier level, both the franchisee and franchisor could have direct liability as a part of the distribution chain. But that question will largely be answered by what the applicable state(s) law provides.[245]

As a threshold matter, parties will want to determine whether the injury was sustained in a state that imposes strict liability on restaurants that serve contaminated or adulterated food. Many states have held that the sale of food is governed by the principles of strict products liability or warranty laws imposed by the Uniform Commercial Code.[246] In New Jersey, for example, restaurants are held to a strict liability standard:

> The service of food in a restaurant is a sale. And a restaurant which sells the food to its customers warrants that the food will not be foul. The sale of food in a restaurant therefore fits perfectly within the UCC definition of the implied warranty of merchantability. The restaurant is thus strictly liable to the plaintiffs.[247]

Other states, however, require proof of fault to hold a party liable for the sale of contaminated food and apply common law tort principles to determine liability in cases of foodborne illness outbreaks.[248] In states requiring proof of fault, customers must show that the restaurant selling the contaminated food owed them a duty and was negligent in performing that duty.

Insofar as franchisors in particular are concerned, the question of liability generally comes down to the franchisor's actual or perceived control over the products, franchise operations, and the public's reliance on the franchisor's express or implied warranty – particularly where the franchisor selects or approves the supplier of the adulterated food product.[249] However: "In some

---

[245] This paper discusses U.S.-based foodborne illnesses only. International laws and regulations would of course need to be considered for non-U.S. incidents.

[246] *See* Wachtel v. Rosol, 159 Conn. 496, 499, 271 A.2d 84, 85–86 (1970); Koster v. Scotch Assocs., 273 N.J. Super. 102, 107, 640 A.2d 1225, 1228 (N.J. Super. Ct. Law. Div. 1993); Hebert v. Loveless, 474 S.W.2d 732, 737 (Tex. Civ. App. 1971), *writ refused N.R.E.* (Apr. 5, 1972).

[247] *Scotch Assocs.*, 273 N.J. Super. at 107, 640 A.2d at 1228.

[248] *See, e.g.,* Chambers-Johnson v. Applebee's Rest., 101 So. 3d 473, 476–77 (La. Ct. App. 2012), (holding that under Louisiana law "the proper analysis to determine a restaurant's liability for foreign substances or things found in food is the traditional duty-risk tort analysis. Under this analysis, the plaintiff must prove: (1) a duty; (2) a breach of that duty; (3) cause-in-fact; (4) scope of liability or scope of protection; and (5) damages"); *see also,* Cain v. Sheraton Perimeter Park S. Hotel, 592 So. 2d 218, 220 (Ala. 1991).

[249] Kosters v. Seven-Up Co., 595 F.2d 347, 353 (6th Cir. 1979) ("When a franchisor consents to the distribution of a defective product bearing its name, the obligation of the franchisor to compensate the injured consumer for breach of implied warranty, we think, arises from several factors in combination: (1) the risk created by approving for distribution an unsafe product likely to cause injury, (2) the franchisor's ability and opportunity to eliminate the unsafe character of the product and prevent the loss, (3) the consumer's lack of knowledge of the danger, and (4) the consumer's reliance on the trade name which gives the intended impression that the franchisor is responsible for and stands behind the

instances, the franchisor may not retain the right of control or may not actually approve the form of the product. The franchisee may sell a product contrary to the instructions or without the knowledge of the franchisor."[250] In those instances, the franchisor's liability will depend on traditional theories of agency and apparent authority.[251] These inquiries are always fact based and "a disclaimer of agency in a franchise agreement will not, by itself, defeat liability where the circumstances indicate that the requisite control exists."[252]

Courts have differences of opinion as to whether the right to control a franchisee granted through a franchise agreement is sufficient to result in such liability. For example, in 2010, the Georgia Court of Appeals found that franchisor Schlotzsky's Deli was entitled to summary judgment on a claim by consumers alleging that they had contracted hepatitis after eating at a franchise location.[253] The court held that the mere fact that the franchise agreement and operations manual provided details regarding food safety standards was not enough to make the franchisee an alter ego of the franchisor.[254] Likewise, the fact that the franchisor gave the franchisee advice related to handling the media was insufficient to overcome the franchisor's motion for summary judgment regarding lack of agency.[255]

Conversely, in 1998, the Oregon Court of Appeals found that a triable question of fact precluded summary judgment on whether a franchisor was liable to a plaintiff who found a blue sapphire in her hamburger when eating at a McDonald's restaurant.[256] The court found particularly relevant that the franchise agreement and the operations manual laid out specific operational requirements that the plaintiff alleged were deficient and resulted in her injury.[257] Further, the court found that the franchise agreement required the franchisee to identify itself as associated with the franchisor's brand, which the plaintiff alleged resulted in her belief that the franchisor controlled those operations.[258] Thus, the court reasoned an objective jury could find that the plaintiff reasonably relied upon the franchisee's apparent authority to act as the franchisor's agent in serving the contaminated hamburger, and therefore the franchisor could be vicariously liable to her.[259]

---

product. Liability is based on the franchisor's control and the public's assumption, induced by the franchisor's conduct, that it does in fact control and vouch for the product."); Bartholomew v. Burger King Corp., 15 F. Supp. 3d 1043, 1048 (D. Haw. 2014) ("Many cases from other jurisdictions . . . describe the well-accepted general principles of franchisor liability—franchisors may be liable where they control or have the right to control day-to-day operations of the franchisee sufficient to establish an agency relationship.").

[250] *Seven-Up Co.*, 595 F.2d at 352.

[251] *Id.*

[252] *Bartholomew*, 15 F. Supp. 3d at 1049.

[253] Schlotzsky's, Inc. v. Hyde, 538 S.E.2d 561, 562-63 (Ga. Ct. App. 2000).

[254] *Id.* at 562.

[255] *Id.* at 563.

[256] Miller v. McDonald's Corp., 945 P.2d 1107, 1108 (Or. Ct. App. 1997).

[257] *Id.* at 1111.

[258] *Id.* at 1112-13.

[259] *Id.* at 1109-10.

2. Franchisor liability to franchisees

Although there are few reported cases on the topic, franchisees may also hold a franchisor liable if an outbreak or contamination results from the franchisor's actions. For example, in June 2019, a group of Michel's Patisserie franchisees in Australia announced their intent to file a class action lawsuit against franchisor Retail Food Group ("RFG") over losses resulting from RFG's instructions to franchisees to extend the use-by dates on certain food items.[260] Most often these claims will depend on the contractual indemnification language in the franchise agreement[261], although tort claims may also be available. Generally, however, franchise agreements limit a franchisor's contractual indemnification responsibilities for foodborne illness to cases where the franchisor itself is the supplier.[262]

3. Liability of officers and directors of franchise systems

While a franchisor may wish to limit its control over operations to avoid vicarious liability, doing so when it comes to food safety may have an adverse personal impact on the individuals in charge. Officers and directors may face both civil and criminal liability for failure to adequately police food safety in a franchise system. For example, officers and directors may face derivative actions by shareholders in the event of an outbreak. In some instances, those actions are premised on the officers' and directors' failures to adequately implement prophylactic measures to protect the brand from outbreaks.[263] In other instances, the claims may be based on a failure by the officers and directors to properly disclose the risks to the shareholders.[264] In either case, officers and directors must be careful to weigh food safety risks when considering how to police the brand and what to share with their shareholders about those potential risks.

Further, officers and directors may also face criminal liability for failing to implement adequate procedures to prevent the distribution of contaminated food into the stream of commerce. Under the Food, Drug and Cosmetics Act as set forth in 21 U.S.C. § 331, *et seq.* (the "FDCA"), individuals are prohibited from "causing" the adulteration or misbranding of food or "causing" the introduction or delivery of an adulterated or misbranded food product into interstate commerce. Pursuant to 21 U.S.C. § 333(a)(1), a person who violates this Act is guilty of a misdemeanor with a punishment of up to one year in prison or a $1,000.00 fine, or both. Pursuant

---

[260] Dominic Powell, *Retail Food Group faces new class action lawsuit from Michel's Patisserie franchisees, alleging loss and damages*, SMARTCOMPANY (June 17, 2019), https://www.smartcompany.com.au/business-advice/franchising/retail-food-group-class-action/.

[261] *See generally* W. MICHAEL GARNER, 1 FRANCH. & DISTR. LAW & PRAC. § 3:38 (Clark Boardman Callaghan 2019-2020 ed. 2019).

[262] *Id.*

[263] *See* Marchand v. Barnhill, 212 A.3d 805 (Del. Sup. Ct. 2019) (holding that directors and officers of food and beverage companies have a responsibility to ensure that they regularly consider food safety compliance measures as a board and require management to report any failures to the board for it to address); *see also*, Nicole Banas, *Chipotle Execs Agree to Settle Derivative Suit Over Illness Outbreaks*, 33 NO. 8 WESTLAW J. CORP. OFFICERS AND DIRECTORS LIABILITY 7, 7 (also available online at 2017 WL 4621980, at *1) ("Chipotle Mexican Grill Inc. directors have agreed to settle a consolidated shareholder derivative lawsuit alleging they allowed lax food safety standards that led to widespread foodborne illness outbreaks at the company's restaurants in 2015.").

[264] *See generally* Ong v. Chipotle Mexican Grill, Inc., 329 F.R.D. 43, 47 (S.D.N.Y. 2018) (appeal filed).

to 21 U.S.C. § 333(a)(2), a person who violates the act with an intent to defraud or mislead is guilty of a felony with a punishment of up to three years in prison or a $10,000.00 fine, or both.

> Under the FDCA responsible corporate officer concept, individuals who by reason of their position in the corporation have the responsibility and authority to take necessary measures to prevent or remedy violations of the FDCA and fail to do so, may be held criminally liable as responsible corporate agents, regardless of whether they were aware of or intended to cause the violation. The FDCA punishes neglect where the law requires care, or inaction where it imposes a duty because according to Congress, the public interest in the purity of its food is so great as to warrant the imposition of the highest standard of care on distributors. A corporate officer may avoid liability under this doctrine by showing that he was powerless to prevent or correct the violation.[265]

Therefore, in addition to the brand risks caused by not implementing proper food safety procedures, such failures could also create risks to individual officers and directors. For example, Blue Bell Creameries' officers and directors faced civil and criminal actions following a listeria outbreak in 2015, which caused eight people to fall ill, three of whom ultimately died.[266] An investigation revealed that the food safety problems at Blue Bell were apparently well-known to the top officers of the company who never disclosed the problems to the board; and the board never inquired about the company's food safety measures.[267] As a result of these failures, not only did the directors face a derivative suit alleging breaches of fiduciary duty, but the company's former president and chief executive officer was indicted on seven felony counts in an action by the United States Department of Justice alleging that he covered up the 2015 outbreak and failed to inform customers of the dangers.[268] The company also entered into a plea agreement whereby it plead guilty to two misdemeanor counts of distributing adulterated food products, and agreed to pay criminal fines and civil penalties in the amount of $19.35 million.[269] Officers and directors of all food and beverage companies should heed these risks as they consider how their companies respond to food safety concerns.

4. <u>Suppliers' liability to a franchise system</u>

The good news for franchise systems is that they are not alone in the fight over food safety. Where a foodborne illness outbreak results from the failure of a supplier, a brand may have direct recourse against the supplier. Generally these claims will be based on theories of breach of

---

[265] United States v. DeCoster, 828 F.3d 626, 632 (8th Cir. 2016), *cert. denied*, 137 S. Ct. 2160, 198 L. Ed. 2d 232 (2017) (internal citations and quotations omitted) (upholding three-month sentence of officers who were "habitual violators" of environmental laws).

[266] *Marchand,* 212 A.3d at 814.

[267] *Id.* at 811-12.

[268] Blue Bell Creameries Agrees to Plead Guilty and Pay $19.35 Million for Ice Cream Listeria Contamination – Former Company President Charged, THE UNITED STATES DEPARTMENT OF JUSTICE (May 1, 2020), https://www.justice.gov/opa/pr/blue-bell-creameries-agrees-plead-guilty-and-pay-1935-million-ice-cream-listeria.

[269] *Id.*

implied or express warranties or contractual indemnification obligations.[270] As further discussed below, franchisors and franchisees will need to act quickly to gather evidence that the food product was contaminated at the supplier level and was not the result of any act or omission by the restaurant itself.[271]

With advancements in technology, however, tracking outbreaks and gathering evidence of the source of the outbreak may become easier. Blockchain technology, first implemented in the cryptocurrency arena with Bitcoin, records data about individual food supply purchases, including origin and expiration date.[272] These individual pieces of data are combined to create a chain of events allowing food retailers and restaurants to track the source of contaminated food products. Ultimately, Blockchain gives food retailers and restaurants the ability to identify the source of both regional and national outbreaks and quickly respond by pulling products from contaminated suppliers.[273] For instance, beginning in August 2017, Walmart began a partnership with IBM to create a platform for tracking its food supply, and in 2019 began requiring both direct suppliers and their related farms to supply relevant data related to its purchases.[274]

B. Navigating a Minefield – Responding to a Public Health Threat

Once a foodborne illness has hit a franchise system, franchisors and franchisees alike must react quickly to ensure they meet all their legal obligations, mitigate the negative impact on the brand, and preserve any cause of action they may have against third parties. This section discusses considerations franchisors and franchisees should make in responding to the first sign of a public health threat.

1. Notice to consumers

Franchisors and franchisees should be aware that some states may impose a duty to warn customers of the danger of a product purchased before and even after a sale. Some states, for example, may require warnings on menus regarding known risks, such as the risk of eating raw proteins.[275] A restaurant's failure to abide by these statutes or regulations could result in liability to a sick consumer if the failure to warn is the cause of the customer's injury.[276] In many states,

---

[270] *See generally* Cohron v. Wendy's Int'l, Inc., No. 1:06-CV-146 TS, 2008 WL 2149386 (D. Utah May 20, 2008); Vons Companies, Inc. v. Seabest Foods, Inc., 926 P.2d 1085 (Cal. 1996); Hebert v. Loveless, 474 S.W.2d 732, 738 (Tex. Civ. App. 1971), *writ refused N.R.E.* (Apr. 5, 1972); Estate of Kriefall v. Sizzler USA Franchise, Inc., 816 N.W.2d 853 (Wis. 2012).

[271] *Hebert*, 474 S.W.2d at 738 ("As to the ice company, however, its liability is slightly different. It delivered the ice to the restaurant and the burden was upon the patron and the restaurant owner, if either were to prevail, to show that it was defective or unfit for its use at the time of delivery.").

[272] Walter G. Johnson, *Blockchain Meets Genomics: Governance Considerations for Promoting Food Safety and Public Health*, 15 J. FOOD L. & POL'Y 74, 87 (2019).

[273] *Id.*

[274] *Id.*

[275] *See, e.g.,* FLA. ADMIN. CODE ANN. r. 64D-3.040; 51 LA. ADMIN. CODE tit. IX, § 319.

[276] *See, e.g.,* Vargas v. Cont'l Cuisine, Inc., 900 So. 2d 208, 211 (La. Ct. App. 2005) ("In this case, the DHH clearly failed in its duty under the Sanitary Code to ensure that the restaurant posted adequate warnings on its menus and above the bar. The question remains, however, whether the defendant's breach of duty was the cause-in-fact of plaintiff's injury.").

the duty to warn arises only if the dangerous condition is known at the time of the sale.[277] For example, if a restaurant is aware of a particular risk at the time of sale based on a distributor's warning, the restaurant may have a duty to share the warning with the consumer.[278] Other states, however, impose a duty to warn a customer even after the danger is discovered, particularly where a warning could prevent further injury.[279] When it comes to a post-sale duty to warn of contaminated food, franchisors and franchisees will want to know the prophylactic window for prevention of particular foodborne illnesses. For example, some illnesses, such as hepatitis A, can be prevented post-exposure if a vaccine is received within two weeks of exposure. Knowing if there is a post-exposure prophylactic window for treatment, and how long the window is, may impact a restaurant's decision to warn the public and when. Even if there is no post-exposure prophylactic window for medical treatment, restaurants may wish to nevertheless warn consumers as a part of their crisis management and customer service protocols. Of course, the tension with warning the public is that often times, trace-back investigations to confirm the source of the outbreak may be incomplete or inconclusive by the time the prophylactic window expires. Warning the public of a potential foodborne illness outbreak prematurely carries its own set of public health and business risks, particularly if the threat turns out to be a false alarm. For this reason, whenever a foodborne illness is suspected or threatened, restaurants should work closely with public health officials and follow their guidance.

2. Notifying insurance carriers

Most franchisors and franchisees will have insurance to cover many direct losses from foodborne illness contamination, such as coverage for personal injury claims or damage suffered as a result of unusable inventory.[280] These policies may also cover business interruption losses resulting from the contamination; however many insurance companies may require that insureds obtain stand-alone business interruption or tradename restoration policies to protect against economic losses, such as loss to reputation or goodwill.[281] In any instance, most insurance policies will require the claimant to notify the carrier of a potential claim immediately or within a short time frame after discovery in order to maintain coverage. And some policies may restrict what the restaurant can communicate to consumers or the type of relief that may be offered to

---

[277] *See, e.g.,* Kimmel v. Clark Equip. Co., 773 F. Supp. 828, 831 (W.D. Va. 1991); Ambrose v. Southworth Prods. Corp., 953 F. Supp. 728 (W.D. Va. 1997); *but see* McAlpin v. Leeds & Northrup Co., 912 F. Supp. 207 (W.D. Va. 1996); Powell v. Diehl Woodworking & Machinery, Inc., 198 F. Supp.3d 628 (E.D. Va. 2016); Rash v. Styker Corp., 589 F. Supp. 2d 733 (W.D. Va. 2008); In Re: General Motors LLC Ignition Switch Litigation, 202 F. Supp. 3d 362 (S.D.N.Y. 2016) (forecasting Virginia law).

[278] *See, e.g.,* Edwards v. Hop Sin, Inc., 140 S.W.3d 13, 17 (Ky. Ct. App. 2003), as modified (Sept. 19, 2003) (holding that a jury could find that a restaurant caused injury to the plaintiff resulting from eating raw oysters where the restaurant received a package containing a manufacturer's warning regarding the risks and the restaurant did not pass that warning on to the plaintiff).

[279] *See, e.g.,* Lunghi v. Clark Equipment Co. 153 Cal. App. 3d 485, 494 (1984) (providing for a post-sale duty to warn if the product is discovered to have dangerous propensities); DeLoach v. Rovema Corp., 241 Ga. App. 802, 804, 527 S.E.2d 882, 883 (2000) ("Georgia law recognizes a manufacturer's duty to warn consumers of danger arising from the use of a product based on knowledge acquired after the product is sold. But Georgia law imposes a duty on a seller to warn only of dangers actually or constructively known at the time of the sale.").

[280] Marc S. Mayerson, *Insurance Recovery for Losses from Contaminated or Genetically Modified Foods*, 39 TORT TRIAL & INS. PRAC. L.J. 837, 848 (2004); *see also* Nat'l Union Fire Ins. Co. of Pittsburgh, PA v. Ready Pac Foods, Inc., 782 F. Supp. 2d 1047, 1055 (C.D. Cal. 2011) (rejecting a claim by Taco Bell for insurance recovery to cover lost profits caused by a loss of customers following a foodborne illness outbreak because those damages were not directly caused by the contaminated food or an essential expense incurred in addressing the contamination).

[281] Mayerson, *supra* note 280, at 852-53.

consumers (such as refunds) in order to maintain coverage. Therefore, a franchisor or franchisee facing a foodborne illness threat should immediately review its insurance policy (and consider retaining coverage counsel) to ensure that it does not take any action which could compromise coverage.

3. Impact of Communications on Attorney Client Privilege

The attorney-client privilege can be difficult to maintain, but never more so than during a crisis. When facing a foodborne illness outbreak, a franchise system may have many members on its crisis response team, including business leaders, attorneys, communication experts, public relations consultants, media personnel, insurance experts, and medical professionals. In addition, franchisors will have frequent communications with franchisees, customers, suppliers and public health officials. Franchisors and franchisees alike will want to be careful about how it shares legal advice and communicates with each of these crisis team members and stakeholders in order to avoid waiving the attorney-client privilege.

a. Communications with franchisees and suppliers

Communications with affected franchisees and suppliers are unlikely to be privileged in any stage of litigation, but particularly in early stages. Generally, sharing privileged communications with a third-party waives the attorney-client privilege. However, "[t]he joint defense privilege, more properly identified as the 'common interest rule,' has been described as an extension of the attorney client privilege."[282] The doctrine allows represented parties who share a common legal interest to share privileged information with each other in order to obtain legal advice without waiving the privilege.[283] To assert that communications are privileged as a result of the common interest doctrine, the party must show: "1) the communication was made by separate parties in the course of a matter of common interest, 2) the communication was designed to further that effort, and 3) the privilege has not been waived."[284] If the parties share only purely commercial interests, then the common interest doctrine will generally not apply; however, the doctrine may still apply if the parties share commercial interests in addition to "substantial legal

[282] United States v. Schwimmer, 892 F.2d 237, 243 (2d Cir. 1989). The terms joint defense privilege and common interest privilege are generally used interchangeably by courts, however, some courts may distinguish between the two, applying "joint defense" only to instances where litigation is ongoing and "common interest" to other situations. *See* Regents of Univ. of California v. Affymetrix, Inc., 326 F.R.D. 275, 279 (S.D. Cal. 2018) ("The 'common interest' or 'joint defense' doctrine is an exception to the general rule that disclosure of protected material to third parties constitutes a waiver."); United States v. Gonzalez, 669 F.3d 974, 978 (9th Cir. 2012) ("The [joint defense] privilege is also referred to as the 'common interest' privilege or doctrine, because it has not been limited to criminal defense situations or even situations in which litigation has commenced."); *but see* In re Grand Jury Subpoena, 274 F.3d 563, 572 (1st Cir. 2001) ("The joint defense privilege protects communications between an individual and an attorney for another when the communications are part of an ongoing and joint effort to set up a common defense strategy. Because the privilege sometimes may apply outside the context of actual litigation, what the parties call a 'joint defense' privilege is more aptly termed the 'common interest' rule." (internal quotations and citations omitted)); *see also* PAUL R. RICE ET AL., ATTORNEY-CLIENT PRIVILEGE IN THE U.S. § 4:35 (Lawyers Cooperative Publishing 2019-2020 ed. 2019) ("The 'community of interest' rule is distinguished from the 'joint defense' rule by the fact that the collaboration between the parties need not be related to a pending legal action."). For purposes of this paper, we will refer to the terms interchangeably.

[283] *Schwimmer*, 892 F.2d at 243; Sedlacek v. Morgan Whitney Trading Grp., Inc., 795 F. Supp. 329, 331 (C.D. Cal. 1992).

[284] In re Mortgage & Realty Trust, 212 B.R. 649, 653 (Bankr. C.D. Cal. 1997), citing In re Bevill, Bresler & Schulman Asset Management Corp., 805 F2d 120, 126 (3d Cir. 1986).

interests."[285] Even in that instance, however, if the communications are to discuss business strategy, rather than legal strategy, then the common interest doctrine will not apply, unless the business communications are "infused with legal concerns."[286]

In the early stages of a crisis, the uncertainty as to future litigation can also have an impact on the privilege. There is no clear determination by most jurisdictions as to whether there must be anticipated or pending litigation for the common interest doctrine to apply. Some courts require that for the common interest doctrine to apply, the communication must be shared in furtherance of a common legal interest in "pending or reasonably anticipated litigation."[287] However, other courts do not require that a lawsuit is or ever will be pending in order to invoke the common interest doctrine.[288]

Finally, the parties' future interests may diverge in litigation due to disputes over the scope of liability of each party, creating conflicts over information previously shared by the parties. Therefore, franchisors and franchisees alike may be best served by retaining separate counsel and avoiding sharing privileged communications with one another or with any supplier. If, however, franchisors or franchisees wish to pursue a common defense or share privileged information with each other or a third party, it is recommended, but not required, that they execute a joint defense agreement setting forth the terms of the collaboration in order to document the parameters of the agreement and the parties' intentions.[289] Further, parties with a shared common interest privilege should avoid mixing business discussions with legal discussions to avoid waiver of the privilege.

b. <u>Communications with insurers and public relations firms</u>

In sharing information with an insurance company, a franchisor and franchisee will want to be mindful of potential coverage disputes. Often times, a carrier provides a defense subject to a reservation of rights, including the right to rescind coverage if the facts later show that the

---

[285] Audi of Am., Inc. v. Bronsberg & Hughes Pontiac, Inc., No. 3:16-CV-2470, 2017 WL 2480588, at *2 (M.D. Pa. June 8, 2017).

[286] MobileMedia Ideas LLC v. Apple Inc., 890 F. Supp. 2d 508, 515 (D. Del. 2012); *see also* In re Federal Trade Commission, No. M18-304 (RJW), 2001 WL 396522, at *3 (S.D.N.Y. Apr. 19, 2001) ("Only communications made in the course of an ongoing legal enterprise, and intended to further the enterprise, are protected. However, it is not necessary that there be actual litigation in progress for the common interest rule to apply. The parties among whom information is shared must have a common legal interest—they must have demonstrated cooperation in formulating a common legal strategy. The rule does not encompass a joint business strategy which happens to include as one of its elements a concern about litigation." (internal quotations and citations omitted)).

[287] United States v. Duke Energy Corp., 214 F.R.D. 383, 388 (M.D.N.C. 2003), aff'd, No. 1:00CV1262, 2012 WL 1565228 (M.D.N.C. Apr. 30, 2012) ("It is concluded that in order for the attorney-client privilege to be expanded by the joint defense/common interest rule, Duke Energy must show an agreement among all members of the UARG to share information as a result of a common legal interest relating to ongoing or contemplated litigation."); Kenyon & Kenyon LLP v. SightSound Techs., LLC, 151 A.D.3d 530, 531, 58 N.Y.S.3d 298, 299 (N.Y. App. Div. 2017).

[288] *Grand Jury*, 274 F.3d at 572; *Schwimmer*, 892 F.2d at 243; Jones v. Tauber & Balser, P.C., 503 B.R. 510, 518 (N.D. Ga. 2013).

[289] *Gonzalez*, 669 F.3d at 979 ("[I]t is clear that no written agreement is required, and that a [joint defense agreement] may be implied from conduct and situation, such as attorneys exchanging confidential communications from clients who are or potentially may be codefendants or have common interests in litigation."); *see also* United States v. Agnello, 135 F. Supp. 2d 380, 382 (E.D.N.Y.), aff'd, 16 F. App'x 57 (2d Cir. 2001) (analyzing the sufficiency of the evidence of an implied joint defense agreement where no written agreement existed).

incident is not a covered event.[290] In those cases, a franchisor and franchisee may want to avoid sharing privileged information with its insurer to avoid any waiver of privilege in a later coverage dispute.[291] Similarly, a franchisor may retain an outside public relations firm to assist with its response. Courts are split on whether communications with a public relations firm, even if hired directly by counsel, remain privileged.[292] Ultimately, while a quick response is necessary to protect a franchise system in the wake of a foodborne illness crisis, franchisors and franchisees alike must act with caution in their actions and communications to avoid future issues in litigation.

C. The Foodborne Illness Litigation Landscape

Even with a swift response, a franchise system may face litigation with consumers, suppliers, and franchisees in the wake of a foodborne illness crisis. This section will discuss some of the various litigation concerns, such as exposure to class action lawsuits, potential coverage disputes with insurers, and recovery from suppliers who are the cause of economic losses suffered by the franchise system.

1. Exposure to class action lawsuits by consumers

Generally, franchise systems should be able to avoid class action lawsuits by consumers for foodborne illness injuries. The Advisory Committee Notes to the 1966 Amendment to Rule 23(b)(3) expressly state that a mass tort claim is "ordinarily not appropriate for a class action." Further, *in Amchem Prods., Inc. v. Windsor*, 521 U.S. 591, 625 (1997), the United States Supreme Court held that personal injury actions based upon products liability are not suitable for class certification because they "present 'significant questions, not only of damages but of liability and defenses of liability. . . affecting individuals in different ways.'"[293] Likewise, in a case arising in an Indiana district court following *Amchem*, the court granted the defendants' motion to strike the plaintiffs' nationwide class allegations for personal injury claims, noting that, since *Amchem*, "no federal appellate court has approved a nationwide personal injury, product liability or medical monitoring class."[294]

---

[290] Rockwell Internat. Corp. v. Superior Court, 32 Cal. Rptr. 2d 153, 158 (Cal. App.1994).

[291] *Id.*

[292] *Grand Canyon Skywalk*, 2015 WL 4773585, at *9 ("Courts are divided on whether the attorney-client privilege extends to communications between a client's counsel and a public relations consultant that the client or its counsel hires to assist in ongoing or anticipated legal matters or disputes. In support of its position, Gallagher & Kennedy relies on In re Grand Jury Subpoenas Dated March 24, 2003 ("In re Grand Jury Subpoenas"), 265 F.Supp.2d 321 (S.D.N.Y. 2003); F.T.C. v. Glaxosmithkline, 294 F.3d 141 (D.C. Cir. 2002); and In re Copper Market Antitrust Litigation, 200 F.R.D. 213 (S.D.N.Y. 2001). In opposing the application of the privilege, Plaintiffs rely on Scott v. Chipotle Mexican Grill Inc., 2015 WL 1424009, *3 (S.D.N.Y. 2015); Egiazaryan v. Zalmayev, 290 F.R.D. 421, 431 (S.D.N.Y. 2013); Calvin Klein Trademark Trust v. Wachner, 198 F.R.D. 53, 54–55 (S.D.N.Y. 2000); Fine v. ESPN, Inc., 2015 WL 3447690, *11 (N.D.N.Y. 2015); and McNamee v. Clemens, 2013 WL 6572899, *1, 6 (E.D.N.Y. 2013). The decisions cited by the parties chiefly emanate from federal district courts in New York. The Court has found two decisions from federal districts in other circuits that also address this issue. See Hadjih v. Evenflo Company, Inc., 2012 WL 1957302 (D. Colo.2012); and Schaeffer v. Gregory Village Partners, L.P., 2015 WL 349039 (N.D. Cal. 2015).").

[293] *Id.* (quoting Advisory Committee Notes to the 1966 Amendment to FED. R. CIV. P. 23(b)(3)).

[294] DuRocher v. National Collegiate Athletic Ass'n, No. 1:13-cv-01570, 2015 WL 1505675, *10 (S. D. Ind. Mar. 31, 2015); *see also* In re Vioxx Prods. Liab. Litig., 239 F.R.D. 450 (E.D. La. 2006) (denying certification of nationwide personal injury and wrongful death class); Norwood v. Raytheon Co., 237 F.R.D. 581 (W.D. Tex. 2006) (denying certification of personal injury class on predominance and superiority grounds); Kemp v. Metabolife Int'l, Inc., No. CIV. 00-3513, 2002 WL 113894, at *3 (E.D. La. Jan. 25, 2002) (noting that product liability cases generally do not meet

2. Indemnification duties of suppliers and recovery of economic losses

Where the cause of a foodborne illness results from a supplier, a franchisor or franchisee will generally have a claim against the supplier for indemnification against any personal injury claims arising out of the outbreak.[295] However, recovery for economic losses likely will depend on the terms of any indemnification provisions in the contract with the supplier. As a general rule, most actions against suppliers will arise under the contract between the supplier and the franchisor or franchisee. A breach of a duty which arises under the provisions of a contract between the parties must be redressed under contract, and a tort action will not lie.

Most states generally hold that absent privity of contract, a plaintiff cannot recover economic losses on a negligence theory.[296] The "economic loss rule," known in other jurisdictions by other names, such as the "contort" or "gist of the action" doctrine,[297] generally provides that a contracting party who suffers purely economic losses must seek its remedy in contract and not in tort. Under the economic loss rule, a plaintiff can recover in tort only those economic losses resulting from injury to his or her person or property; a plaintiff cannot recover economic losses associated with injury to the person or property of another.[298] Economic losses may be recoverable under tort theories other than negligence, such as fraud.[299]

3. Insurance coverage requirements and coverage disputes

While insurance coverage is controlled by the specific terms of the policy, a commercial general liability policy generally will cover personal injury and property damage resulting from a foodborne illness, even where a foodborne illness results from negligence in manufacturing or production.[300] However, coverage for recalls may not be a given, particularly where a product is recalled voluntarily in an abundance of caution, without any conclusive evidence of contamination. Generally and subject to the terms of the policy, if it can be shown that the recalled products were

---

predominance requirement); Castano v. American Tobacco Co., 84 F.3d 734 (5th Cir. 1996) (denying national products liability class based on predominance and superiority); Norwood v. Raytheon Co., 237 F.R.D. 581 (W.D. Tex. 2006) (denying certification of personal injury class on predominance and superiority grounds); In re Methyl Tertiary Butyl Ether (MTBE) Prods. Liab. Litig., 437 F. Supp. 2d 298 (S.D.N.Y. 2006) (denying certification of personal injury class on predominance grounds).

[295] *Hebert*, 474 S.W.2d at 738.

[296] Beard Plumbing & Heating, Inc. v. Thompson Plastics, Inc., 152 F.3d 313, 316 (4th Cir. 1998); Taco John's of Huron, Inc. v. Bix Produce Co., LLC, No. CIV. 07-4134-KES, 2008 WL 11450655, at *4 (D.S.D. Sept. 18, 2008); Gen. Elec. Co. v. Lowe's Home Centers, Inc., 608 S.E.2d 636, 637 (Ga. 2005); Hyundai Motor Am., Inc. v. Goodin, 822 N.E.2d 947, 958 (Ind. 2005).

[297] *See, e.g.,* SPP SWD Burns Ranch, LLC v. Kent, No. 5:14-CV-88, 2015 WL 12841097, at *2 (S.D. Tex. Jan. 8, 2015) ("Thereby they argue that any alleged torts merely arise from a breach of the parties' contract and thus that the conversion claim against Rutherford is categorically barred by the 'independent injury' or 'economic loss' rule, otherwise known as the 'contort doctrine.'"); *see also* eToll, Inc. v. Elias/Savion Advert., Inc., 811 A.2d 10, 14 (Pa. 2002) (holding that the gist of the action doctrine is "designed to maintain the conceptual distinction between breach of contract claims and tort claims. As a practical matter, the doctrine precludes plaintiffs from re-casting ordinary breach of contract claims into tort claims." (internal citations omitted)).

[298] *Id.*

[299] Christian C. Burden & Sean Trende, *The Economic Loss Rule and Franchise Attorneys*, 27 FRANCHISE L.J. 192, 194 (2008) (describing the split among courts on whether the economic loss rule limits damages for fraud).

[300] Mayerson, *supra* note 280, at 848-49.

not in fact contaminated, an insurer will not be required to cover any resulting losses.[301] Other exclusions could apply if the coverage is limited to unintentional contamination, and the contamination results from a rogue employee who intentionally contaminated the product.

D. Preparing for an Outbreak

In the case of foodborne illness outbreaks, the best defense is preparation. A prepared franchise system will have robust and protective supplier contracts, thorough distribution and food handling protocols, and a well-thought-out recall and crisis plan.

1. Robust supply chain agreements

Many foodborne illness outbreaks affecting franchise systems are the result of a failure in the supply chain. Vetting suppliers is critical. But even the safest supplier is not immune to a contamination event. With an increasing globalization of the supply chain, franchise systems face greater challenges, particularly when sourcing from suppliers located in countries that lack modern food safety regulations. Franchise systems can mitigate their risks by contractually requiring their suppliers to comply with U.S. food safety laws, in addition to the laws of the supplier's location. Drafting supply chain contracts is probably a separate paper in and of itself. However, some important terms to include in supply chain contracts include: permitting unannounced food-safety audits across the supply chain; requiring a modern food tracing and notification system; limiting sourcing to manufacturers and growers that the franchisor approves; requiring adequate insurance coverage and limits, including appropriate additional insureds; and clear indemnity and risk-allocation provisions that protect the franchise system not only from personal injury claims, but also economic losses and reputational harm.

2. Internal preparedness

Supplier contracts are only half the battle. The other half rests with the franchise system's internal preparedness. Having a recall and crisis plan is critical and identifying a crisis team who can quickly execute the plan is paramount. If it takes a franchisor a week to find an epidemiologist, and the post-exposure prophylactic window is only one week, then critical risk mitigation opportunities have been irreparably lost. It is important that franchisors know who their crisis team members will be before a crisis happens. In addition, franchisors will want to review their own insurance policies and consider retaining coverage counsel to ensure that their policies cover the risks and losses that the franchisor expects to be covered. Likewise, franchise agreements and operations manuals should be reviewed to ensure clear terms and guidelines for franchisees to follow in the event of a recall or outbreak, including notification obligations, decontamination protocols, communication plans, and insurance and indemnity requirements.

A foodborne illness outbreak is the worst nightmare for any restaurant. Smart and savvy restaurant brands will mitigate risks contractually, plan for outbreaks proactively, and respond to claims thoughtfully, with a crisis team that protects every angle of an outbreak including the medical response, sanitation response, media response, consumer response, insurance response, legal response and everything in between.

---

[301] See Foster Poultry Farms, Inc. v. Certain Underwriters at Lloyd's, London, No. 1:14-953 WBS SAB, 2016 WL 235211, at *6 (E.D. Cal. Jan. 20, 2016) (describing the state of case law regarding coverage for voluntary recalls).

V. OTHER DISRUPTORS AFFECTING RESTAURANT FRANCHISE SYSTEMS

A. Global pandemics, global warming, and natural disasters

If 2020 has taught us anything, it is that we must be prepared for everything. With the outbreak of COVID-19, as well as recent natural disasters caused by the increasing effects of global warming, restaurants have witnessed just how critical it is to be able to react quickly in times of crisis. Franchise systems have been impacted by slowdowns in supply chains, government shut-down orders, and new health and safety regulations.[302] For example, weathering COVID-19 required many businesses to quickly implement or increase curbside pickup and delivery.[303] And as the country began to reopen, restaurants had to figure out how to do so safely by developing new sanitization measures to keep both its employees and its customers safe.[304] For franchise systems, the challenges were even greater as franchisors needed to ensure that franchisees were complying with these changes on a system-wide basis, while also trying to relieve the burden on operators who were suffering financially.[305]

And as always, with crisis, comes the threat of litigation, bankruptcies, and insurance disputes. For example, less than two months after the COVID-19 crisis hit the U.S., employees of McDonald's franchisees sued both the franchisor and related franchisees alleging a failure to provide personal protective equipment recommended by public health officials to stop the spread of the disease.[306] Further, some franchisors found themselves facing bankruptcy in the wake of the COVID-19 crisis, when shelter-in-place orders forced closures of a large number of outlets and stopped the flow of royalties and franchise fees.[307] Other restaurants are facing coverage disputes with insurers over losses arising from COVID-19.[308] These disputes may mirror some of the coverage disputes that arose following recent natural disasters, where franchisors and franchisees fought insurance companies to gain coverage for economic losses suffered following

---

[302] Bilzin Sumberg, *Setting the Table in a Post-COVID-19 World: The Restaurant Industry Rises Up to Tackle Its Greatest Challenge Yet (and Maybe Ever)*, JD SUPRA (May 14, 2020), https://www.jdsupra.com/legalnews/setting-the-table-in-a-post-covid-19-63934/.

[303] *Id.*

[304] *Id.*; WK Editorial Staff, *McDonald's Employees File Suit, Administrative Complaint Over Unsafe Working Conditions*, WOLTERS KLUWER (May 26, 2020), https://lrus.wolterskluwer.com/news/employment-law-daily/mcdonald-s-employees-file-suit-administrative-complaint-over-unsafe-working-conditions-during-covid-19/112911/ (also available at 2020 WL 2569734) (describing class actions filed by McDonald's employees in Illinois and California alleging that the franchisor and franchisees failed to provide employees with adequate equipment to protect themselves in the wake of the COVID-19 pandemic).

[305] Faegre Drinker Biddle & Reath LLP, *Franchisor Best Practices for COVID-19*, JD SUPRA, (Mar. 20, 2020), https://www.jdsupra.com/legalnews/franchisor-best-practices-for-covid-19-44136/.

[306] *Id.*

[307] *See, e.g.,* In re: Craftworks Parent LLC, No. 20-10475 (Bankr. D. Del. March 3, 2020); In re: GGI Holdings LLC, No. 20-31318 (Bankr.N.D. Tex. May 4, 2020) (where the Gold's Gym franchisor claimed that "no single factor caused more harm to the Debtors' business than the current COVID-19 pandemic, emergency declarations, and corresponding guidelines").

[308] *See, e.g.,* Legal Sea Foods LLC v. Strathmore Insurance Co., No. 20-cv-10850, 2020 WL 2121558 (D. Mass. May 4, 2020) (alleging that its insurance company breached its contractual obligations by refusing coverage for revenue losses resulting from government orders limiting restaurant operations during the COVID-19 pandemic); *see also* Nate Raymond, *Restaurant chain Legal Sea Foods sues insurer over COVID-19 losses*, 30 No. 32 WESTLAW J. INS. COVERAGE 06 (May 15, 2020).

the destruction of franchise locations in the wake of the disaster.[309]

While both franchisors and franchisees are impacted by these crises, franchisors are often in a better position to prepare for them.[310] Some franchisors will choose to further support their franchisees in a crisis by offering royalty abatements or deferrals, assisting with the negotiation of rent relief, and assisting franchisees in navigating programs for government assistance. Using the lessons learned from the COVID-19 pandemic, franchise systems can improve their readiness and position themselves for a quick and strong response to the next crisis.

B. ADA Compliance in emerging technologies

While not as drastic as a global pandemic, emerging technologies, and the government regulation around them can similarly have a significant disruption on a restaurant business. In particular, many franchise systems are facing legal challenges from consumers who allege that new technology is not compliant with the Americans with Disabilities Act (the "ADA"), as it does not provide equal access to individuals who are hearing, vision, or otherwise impaired.[311] Whether the ADA applies to websites and mobile applications, is still an open question from the perspective of the federal government, as the U.S. Department of Justice has yet to issue any specific guidance or rulemaking on the subject. However, in a letter to Congress in 2018, the Department stated its position that the ADA applies to websites for places of public accommodations, like restaurants.[312] Courts are split however on whether "public accommodations" are limited to physical spaces.[313]

Given the lack of clarity, franchisors operating websites and mobile applications on a national basis for themselves and their franchisees, are likely best served by ensuring compliance with the ADA – particularly since businesses whose technology fails to be ADA compliant are strictly liable and face exposure for statutory damages, attorneys' fees and court orders requiring compliance. To address these concerns, franchisors that control the technology of their systems,

---

[309] *See, e.g.,* Lundy Enterprises, LLC v. Wausau Underwriters Ins. Co., No. CV 06-3509-MVL-SS, 2010 WL 11538544 (E.D. La. 2010) (dispute arising out of flood insurance endorsements coverage for certain Pizza Hut franchisees following Hurricane Katrina).

[310] Andrae J. Marrocco, *The Franchisor's COVID-19 Legal Toolkit*, INTERNATIONAL FRANCHISE ASSOCIATION (Apr. 22, 2020), https://www.franchise.org/franchise-information/legal/the-franchisors-covid-19-legal-toolkit.

[311] *See, e.g.,* Robles v. Domino's Pizza, LLC, 913 F.3d 898, 908 (9th Cir.), *cert. denied*, 140 S. Ct. 122, 205 L. Ed. 2d 41 (2019).

[312] Stephen E. Boyd, *Letter to Congressman Ted Budd*, U.S. DEPARTMENT OF JUSTICE (Sept. 25, 2018), https://www.adatitleiii.com/wp-content/uploads/sites/121/2018/10/DOJ-letter-to-congress.pdf.

[313] For courts finding that a website can be a public accommodation independent of any connection to a physical space, *see* Carparts Distrib. Ctr., Inc. v. Auto. Wholesaler's Ass'n of New England, Inc., 37 F.3d 12, 19 (1st Cir. 1994); Nat'l Ass'n of the Deaf v. Netflix, Inc., 869 F. Supp. 2d 196, 200 (D. Mass. 2012); Nat'l Fed'n of the Blind v. Scribd Inc., 97 F. Supp. 3d 565, 576 (D. Vt. 2015); Andrews v. Blick Art Materials, LLC, 268 F. Supp. 3d 381, 393 (E.D.N.Y. 2017); Morgan v. Joint Admin. Bd., Ret. Plan of Pillsbury Co. & Am. Fed'n of Grain Millers, AFL, 268 F.3d 456, 459 (7th Cir. 2001); Doe v. Mut. of Omaha Ins. Co., 179 F.3d 557, 558 (7th Cir. 1999). For courts finding that goods and services provided by a public accommodation such as through a website or mobile application may fall within the ADA if they have a sufficient nexus to a physical location, *see* Gil v. Winn-Dixie Stores, Inc., 257 F. Supp. 3d 1340, 1349 (S.D. Fla. 2017); Haynes v. Dunkin' Donuts LLC, 2018 WL 3634720, at *2 (11th Cir. July 31, 2018); Weyer v. Twentieth Century Fox Film Corp., 198 F.3d 1104, 1114 (9th Cir. 2000); Earll v. eBay, Inc., 599 F. App'x 695, 696 (9th Cir. 2015); Ford v. Schering-Plough Corp., 145 F.3d 601, 614 (3d Cir. 1998); Peoples v. Discover Fin. Servs., Inc., 387 F. App'x 179, 183 (3d Cir. 2010); Parker v. Metro. Life Ins. Co., 121 F.3d 1006, 1010 (6th Cir. 1997).

or franchisees with their own technology, can hire consultants or contractors to audit their technology for ADA compliance. Further, businesses can require ADA compliance in all contracts with technology vendors, and further require indemnification from third parties who fail to meet these standards. Likewise, to the extent a franchisor allows franchisees to develop their own technology, the franchise agreements should specifically require that any such technology be ADA compliant.

C. Emerging Trends in Employee Pay and Benefits

Trends in employee pay and benefits can similarly disrupt a business and trigger a change in the status quo. This section will discuss some of the emerging trends that impact employee compensation and benefits.

1. Advanced Payment Products

With technology making payments faster, and a need to extend credit in smaller amounts to employees in hourly wage positions, technology companies have created solutions that allow workers advanced access to their next paycheck. Many companies have expressed increasing interest in offering these payment options to employees, as studies show that offering such a benefit dramatically reduces turnover.[314] The interest in these services is furthered by the fact that many advanced pay companies offer the services at low or no cost to the employer, depending on whether the employer opts to pay the fees or pass them onto employee participants.[315] As with many products, buyer beware: Many early pay products are complicated financial tools that come with hidden costs and hidden exposure.

The Consumer Financial Protection Bureau (the "CFPB") has stated that some advanced wage providers are payday lenders and must comply with federal payday lending regulations, while other providers do not extend credit and therefore are not covered by lending regulations.[316] The CFPB has not provided any guidance on what characteristics would subject an advanced pay product to payday lending regulations.[317] Further, state payday lending regulations may be more stringent, and apply to providers even where federal regulations do not apply. In fact, eleven states and Puerto Rico have initiated a joint investigation led by the New York Department of Financial Services into advanced pay companies, alleging that the companies are violating payday lending and usury laws by disguising unlawfully high interest rates as tips in their programs.[318] In California, lawmakers are working on legislation to regulate advanced pay

---

[314] Tom Groenfeldt, *Early Access to Wages, a Prized Benefit, Costs Employers Little or Nothing*, Forbes (Apr. 18, 2019), https://www.forbes.com/sites/tomgroenfeldt/2019/04/18/early-access-to-wages-a-prized-benefit-costs-employers-little-or-nothing/#3c81e0d66312 (citing a Harvard Kennedy School of Government study that shows that businesses offering a specific advanced pay product to their employees saw a 19% reduction in turnover).

[315] *Id.*

[316] Stephen T. Middlebrook, *What Business Lawyers Need to Know about Wage Advance Products*, ABA BUSINESS LAW TODAY (Sept. 5, 2019), https://www.americanbar.org/groups/business_law/publications/blt/2019/09/wage-advance.

[317] *Id.*

[318] Dan Ennis, *11 States Look Into the Divide Among Payroll Advance Companies*, BANKINGDIVE (Aug. 8, 2019), https://www.bankingdive.com/news/nydfs-investigate-earnin-payroll-advance/560534/; *Superintendent of Financial Services Linda A. Lacewell Leads Multistate Investigation of the Payroll Advance Industry*, NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES (Aug. 6, 2019), https://www.dfs.ny.gov/reports_and_publications/press_releases/pr1908061.

products, which would place limits on the amount of fees charged and the amount of income advanced.[319] While the bill passed the California Senate, it is now facing criticism from consumer groups that it does not do enough to limit fees and regulate providers.[320]

Further, advanced pay products must comply with state wage-and-hour laws, which may vary dramatically.[321] For example in New York, if an advanced payment assesses interest or charges a fee, it is not considered a wage advance and cannot be reclaimed through payroll deduction.[322] Similarly, some advanced pay products require the employee to assign some or all of their wages to the advanced pay provider, which may be in violation of state law.[323] For example, Ohio limits the assignment of future wages to paying court-ordered spousal or child support.[324]

As franchisors and franchisees consider adopting these products, they must also be careful to navigate the legal minefields that come along with them. Franchisors and franchisees should pay particular attention to contractual obligations to comply with federal and state laws and regulations, as well as ensuring that adequate indemnification provisions are in place to avoid liability for a provider's failure to comply with such laws.

2. Pandemic-triggered changes in state medical leave laws

Just as early pay products have disrupted typical employee compensation models, so too has COVID-19 disrupted typical employee benefit programs and regulations. As businesses began to reopen following the initial impact of COVID-19, many employees were being called back to work before schools and childcare providers had reopened, and while many employees and their families were still facing health threats related to the pandemic. As a result, medical and family leave laws became more important to both employers and employees in determining how to best protect employees and customers, while also protecting businesses. Recognizing the need to expand access to medical and family leave, the federal government passed new legislation requiring employers with fewer than 500 employees to provide two weeks of paid sick leave and ten weeks of partially paid FMLA-qualified leave to employees affected by COVID-19. The sick leave is available to employees who either are sick with COVID-19 or who are under quarantine.[325] The legislation also provided an additional two weeks of leave at two-thirds pay for employees caring for family members affected COVID-19.[326] The expanded FMLA leave is also

---

[319] S. 472, 2019-2020 Reg. Sess. (Cal. 2019).

[320] Kevin Wack, *As California Mulls Rules for Payday Loan Alternative, Rifts Emerge*, AMERICAN BANKER (June 24, 2019), https://www.americanbanker.com/news/as-california-mulls-rules-for-payday-loan-alternative-rifts-emerge.

[321] Middlebrook, *supra* note 316.

[322] N.Y. COMP. CODES R. & REGS. tit. 12, § 195-5.2.

[323] Middlebrook, *supra* note 316.

[324] OHIO REV. CODE ANN. § 1321.32.

[325] *Families First Coronavirus Response Act: Employee Paid Leave Rights*, U.S. DEPT. OF LABOR, https://www.dol.gov/agencies/whd/pandemic/ffcra-employee-paid-leave (last visited Aug. 31, 2020).

[326] *Id.*

available to employees who lost childcare as a result of the pandemic.[327]

In addition, trends are showing that the federal short-term relief is being expanded into long-term relief by some states. For example, in response to COVID-19, New York enacted a temporary emergency paid sick leave law, with a permanent paid sick leave law to take effect in September 2020.[328] And more states may follow. This may impact franchisors and franchisees alike, particularly in the restaurant industry where most workers are paid hourly and may not have employer provided sick or family leave benefits.

Similarly, expanded unemployment benefits under federal COVID-19 legislation may also impact franchisees' ability to maintain a workforce. With the expansion of benefits and the fear of returning to work, some employees may find it more economically beneficial and less risky to refuse to return to work after being recalled by their employers.[329] However, generally a fear of exposure to COVID-19 will not support the continuation of such benefits.[330] Instead, an employee generally must provide additional support, such as a doctor's note, to show that he or she has risk factors related to COVID-19 that are more serious than the average employee.[331] However, because unemployment insurance is governed at the state level, differing state interpretations of the requirements may differ.[332] For example, Kentucky has issued guidance stating that a reasonable fear of COVID-19 may qualify for benefits, unless the employer makes reasonable accommodations or takes steps to reduce that employee's risk.[333] For restaurants, some obvious accommodations, such as teleworking, may be impossible to implement. Therefore, franchisees will need to focus more on increased sanitary and other safety measures to protect employees in order to meet the state requirements.

VI. CONCLUSION

In the coming years, the restaurant industry and restaurant franchise businesses will continue to face significant disruption that will take many forms, some expected and some unexpected. While restaurants cannot predict precisely what the next major disruptor will be, these businesses, and the legal professionals who support them, can take steps now to prepare.

Inside and outside counsel are uniquely positioned to help restaurant brands spot, prepare for, and confront disruption. Legal counsel can help restaurant businesses stay current on emerging disruptors, including disruption posed by regulatory developments and legal risks associated with developing technologies and new business channels. Counsel can help restaurant businesses develop, and importantly, test, emergency preparedness plans targeted at confronting data breaches, illness outbreaks, disasters, and other business interrupters. In addition, counsel can help franchise restaurant businesses survive the next disruption by

---

[327] *Id.*

[328] S. 8091, 2019-2020 Leg. Sess. (NY 2020).

[329] John F. Birmingham Jr. & Jacqueline A. Haduk, *Dealing with Worker Recall Challenges Caused by the Coronavirus Unemployment Benefit Expansions*, NAT'L LAW REV. (May 26, 2020), https://www.natlawreview.com/article/dealing-worker-recall-challenges-caused-coronavirus-unemployment-benefit-expansions.

[330] *Id.*

[331] *Id.*

[332] *Id.*

[333] *Id.*

successfully negotiating for the inclusion of prophylactic measures in new and existing agreements with vendors and incorporating similar measures into franchise system policies and standards. Finally, counsel can help restaurant franchise businesses emerge from disruption by helping the business understand existing insurance policies and their limitations.

In the words of Charles Darwin, “It is not the strongest or the most intelligent who will survive but those who can best manage change.” Business disruptors should no longer be a surprise, but instead should be an expectation. And with planning and preparation, just about any disruptor can not only be overcome, but can present an opportunity for growth and innovation.

Annie Caiola

Annie Caiola is the managing partner of Caiola & Rose, LLC, an Atlanta-based national law firm focused on representing franchisors in regulatory compliance, litigation, real estate, trademarks and bankruptcy. As an experienced trial attorney, Annie has litigated hundreds of franchise disputes enforcing brand standards and post-termination obligations related to intellectual property and noncompetition covenants, while defending claims alleging fraudulent inducement and violation of consumer protections laws. Annie also served as national counsel and crisis quarterback to a franchisor during an international foodborne illness outbreak that led to multi-district mass tort litigation, international litigation related to indemnification and recovery of economic losses, and system-wide insurance coverage disputes.

In addition to serving as outside counsel to franchisors, Annie has also served as in-house General Counsel to many of her clients on an interim basis. In her in-house roles, Annie has served on the executive team, developed franchisee compliance programs, implemented crisis and risk mitigation plans, and spearheaded aggressive franchise growth targets in partnership with chief development officers.

Annie graduated Phi Beta Kappa from the University of North Carolina in Chapel Hill, where she also received her law degree with honors. Before starting her own law firm, Annie was an associate in the complex commercial litigation practice group at Troutman Sanders. Annie has been recognized as a "Rising Star" by Georgia Super Lawyers Magazine, a "Top 40 Under 40" by The Daily Report, and a "Legal Elite" by Franchise Times Magazine. Annie is currently the Vice Chair of the Franchise & Distribution Section of the Georgia Bar and on the Women's Caucus Committee for the ABA Forum on Franchising. Annie's most recent publication was *Protecting Real Estate Rights When the Franchise Relationship Ends*, 37 FRANCHISE L.J. 553 (Spring 2018).

Brittany Johnson

Brittany Johnson is a franchise and licensing attorney at Starbucks Corporation in Seattle, Washington. Ms. Johnson represents Starbucks in domestic and international franchise transactional matters and has helped Starbucks expand throughout Canada, Europe, Asia, and Latin America. She also serves as the lead lawyer for the Starbucks Latin American and Caribbean business unit. In that role, Ms. Johnson is responsible for advising the company on a wide variety of commercial, supply chain, intellectual property, litigation, and technology matters in the region.

Ms. Johnson currently serves as the Young Lawyers Division Liaison to the Forum on Franchising and leads the Young Lawyers Committee. Previously, Ms. Johnson served on the International Division Committee. She is the author of the 2020 *Franchise Lawyer* article "Franchise Brands Hit the Pavement: Legal and Practical Considerations for Expanding Food Businesses Beyond Traditional Brick-and-Mortar."

Ms. Johnson completed her undergraduate degree at the University of Colorado. She received her J.D. from the University of Denver Sturm College of Law, where she was selected as a member of the Order of St. Ives.

Andra Terrell

Andra Terrell received her B.S. from Johns Hopkins University in 1992 and her J.D. from Howard University School of Law in 1995. She is a member of the Maryland Bar. Mrs. Terrell

currently serves as Vice President and Deputy General Counsel for Cajun Operating Company, d/b/a Church's Chicken, at its corporate headquarters in Atlanta, Georgia. She also is a Board member of, and counsel to, the Church's Partners Foundation.

Prior to her tenure at Church's, Mrs. Terrell was the Assistant General Counsel for Luxottica Retail (an Italian eyewear manufacturer and retailer, and the franchisor of more than 600 and operator of 200 Pearle Visions in the United States and Canada, and franchisor of approximately 100 Oakley locations outside the United States), at its corporate office in Mason, Ohio. Mrs. Terrell also served as the General Counsel of Decorating Den Systems, Inc., an Easton, Maryland-based franchisor of home decorating services in the United States and Canada.

Mrs. Terrell is a member of the American Bar Association Forum on Franchising and has been active in the Corporate Counsel Steering Committee and Diversity Caucus, as well as serving as the Liaison to the ABA Commission on Disability Rights. She is also a member of the International Franchise Association ("IFA") and served two terms on its Task Force. Andra co-authored and presented four articles at various ABA Forum on Franchising annual meetings, four articles at various International Franchise Association annual meetings, two Franchise Lawyer articles and co-authored chapters in the Franchise Law Compliance Manual (Jeffrey Brimer, ed. 2d. ed. 2011), and The Annotated Franchise Agreement (Nina Greene, Dawn Newton and Kerry Olson ed. 2018).

4816-2289-6586, v. 1