International Franchise Association
52nd Annual Legal Symposium
May 5-7, 2019
Washington, DC

Digital Transformation in a Franchise System: Keeping Up with the Technology Race within the Bounds of Existing Franchise Agreements

Tanya Morrison
Home Instead, Inc.
Omaha, NE

Charlene Wilson
H & R Block, Inc.
Kansas City, MO

Ashley Williams
The Maids International, Inc.
Omaha, NE

I. Adopting a Change Mindset*

"The pace of change has never been this fast, yet it will never be this slow again."[1] Adapting the fast pace of changing technology can be incredibly difficult for companies. However, if companies cannot adapt and keep up with the pace of changing technologies, they will quickly become obsolete. According to the Small Business Administration (SBA) Office of Advocacy's 2018 Frequently Asked Questions, roughly 80% of small businesses survive the first year.[2] Only about half of small businesses survive past the five-year mark, ranging from 45.4% to 51%. Beyond that, only about one in three small businesses make it past the 10-year mark.[3] In this digital day and age, companies need to adapt with the changing technology landscape in order to survive. Organizations that cannot adapt to the digital world will not exist. If an organization wants to continue to exist, it is critical to adopt a change mindset within their organization.

a. The Fastest and Most Adaptable Companies Win

i. Target Case Study

In the digital era, consumers use technology to help fulfill their shopping needs. Large e-commerce marketplaces like Amazon have shaped the way most consumers acquire goods, making shopping more efficient and convenient. Consumers have come to expect such a shopping experience, and companies like the Target Corporation ("Target") have adopted a change mindset in order to keep up with the technology race in retail. Specifically, Target recently invested more than $7 billion in capital to grow sales, gain market share, and adapt to consumer preferences.[4]

Target has adapted by using technology to enhance its customers' shopping experience. Target is providing these enhancements by utilizing a) Google Express, Target Restock, Shipt, and Drive Up to advance its shipping and delivery methods; b) data analytics; and c) innovative technology.

a. Shipping and Delivery

Target has incorporated new mechanisms to enhance shipping and delivery methods for their shoppers. One way in which Target has done this is through a partnership with Google. Through the partnership, Target shoppers can shop their local Target store using Google Express.[5] Google Express allows consumers to shop from retailers online and have the items delivered to their homes. Orders using this method

* The authors would like to thank Owen Behle, Legal Intern, Home Instead, Inc. and Elizabeth Simpson, Regulatory Counsel, Home Instead, Inc., for their valuable contribution to this paper.

[1] Canadian Prime Minister Justin Trudeau speech at the World Economic Forum in 2018

[2] https://www.sba.gov/sites/default/files/advocacy/Frequently-Asked-Questions-Small-Business-2018.pdf

[3] https://www.forbes.com/sites/forbesfinancecouncil/2018/10/25/what-percentage-of-small-businesses-fail-and-how-can-you-avoid-being-one-of-them/#48ac0d8443b5

[4] https://corporate.target.com/article/2017/02/financial-community-meeting

[5] https://corporate.target.com/article/2017/10/target-google-express

arrive in only two days. If the shopper prefers to physically go to Target, the Google Express order can be picked up from the local Target store and will be ready for pickup in two hours.[6] Moreover, in order to keep up with Amazon's "Alexa," shoppers are now able to shop and order by vocalizing commands using their smartphone or a Google Home device.[7] Through the use of this system, shoppers can shop for approximately 100,000 items from Target by speaking to a device.

Another way that Target has applied new technology to enhance its shipping and delivery methods is through Target Restock. Target Restock is a shipping service that provides next-day delivery of essential household items if the items are ordered before 7 p.m.[8] Target Restock markets itself as providing "everyday essentials" such as groceries, cleaning supplies, and beauty products that can be ordered through the Target Restock website. Target can deliver so quickly because they fulfill the orders using the nearby stores. Furthermore, like Google Express, shoppers can use voice activated smartphones and Google Home devices to place orders using speech.[9]

Target Restock is comparable to Amazon Prime Pantry. However, because of the prevalence of Target stores, Target Restock is able to effectively compete with Amazon Prime Pantry by providing faster shipping. There is no membership requirement or order minimum.[10] To compare, Amazon Prime Pantry costs $4.99 monthly and provides free shipping for orders over $10.[11] Finally, Target Restock's delivery fee is $2.99 or free for consumers using their Target REDCard,[12] while Amazon Prime Pantry's delivery fee is $5.99 on orders under $35, or free on orders over $35.[13]

Target has also adapted to the new technological climate of retail by acquiring a company called Shipt. Shipt is a membership-based grocery market with same-day delivery that allows shoppers to place online orders of food and household essentials from nearby grocery or Target stores.[14] A Shipt "shopper" will hand select the items a customer places in their online order and deliver the items to the customer.[15] Not limited to Target stores, chains including Meijer, Hy-Vee, CVS Pharmacy, Petco and others are adopting Shipt delivery.[16] The official acquisition statement cites Shipt as a wholly owned

---

[6] *Id.*
[7] http://www.startribune.com/target-teams-up-with-google-for-voice-assisted-shopping-and-nationwide-delivery/450595873/
[8] https://corporate.target.com/article/2018/05/nationwide-restock-rollout
[9] *Id.*
[10] https://www.fool.com/investing/2018/05/16/targets-revamped-restock-service-blows-amazon-prim.aspx
[11] https://www.amazon.com/Prime-Pantry/b?ie=UTF8&node=7301146011
[12] https://www.fool.com/investing/2018/05/16/targets-revamped-restock-service-blows-amazon-prim.aspx
[13] https://www.amazon.com/Prime-Pantry/b?ie=UTF8&node=7301146011
[14] https://corporate.target.com/article/2017/12/target-acquires-shipt
[15] https://www.shipt.com/?param=home&noredirect
[16] *Id.*

Target subsidiary with its own team operating independently.[17] The membership fee is $14 per month or $99 per year.[18]

In addition to same-day delivery, Shipt also uses algorithms to enhance customer service. For example, the person who shops for the customer's items is also the person who delivers them. A built in rating system allows customers to give real-time feedback. This feedback is used to pair shoppers with the same delivery person when the feedback rating is high, and not pair them again when the feedback is low.[19]

Additionally, Target has introduced Drive Up to adapt to technological changes in retail. Drive Up allows shoppers to place orders through the Target app, and then have their purchases brought to their car in front of the physical Target location by a staff member.[20] For example, when shopping on the Target app, the shopper can press "Drive Up" as the fulfillment option when placing the order. Then, Target notifies the shopper when the order is ready, which is usually within the hour. Subsequently, the shopper presses the "on the way" button when they are headed to the store. Thereafter, the shopper will park their car in the drive up stop, where the staff member will bring out the order to the car within two minutes.[21]

Finally, Target has also implemented a new technology to minimize shipping costs. The new technology is an application for employees' handheld devices that helps the employee figure out which box size is best for online shipping orders.[22] The application ensures that Target does not waste money on shipping empty space in a box. Furthermore, the application decides which delivery carrier is optimal to use for shipping the order.[23]

b. Data Analytics

Alongside incorporating technology to provide efficient and convenient shipping and delivery, Target has successfully used data analytics to improve its ability to predict and respond to consumer behavior.[24] There are many variables retailers need to weigh in order to make smart decisions. For example, retailers must predict demand in order to plan inventory.[25] They want to have the goods people want, when they want them, and not too much.[26]

---

[17] https://corporate.target.com/article/2017/12/target-acquires-shipt
[18] https://www.businessinsider.com/target-shipt-same-day-grocery-delivery-how-does-it-work-2018-7
[19] https://corporate.target.com/article/2017/12/target-acquires-shipt
[20] https://corporate.target.com/article/2018/08/drive-up-california-colorado
[21] *Id.*
[22] http://www.startribune.com/target-shows-off-new-tech-it-s-developing/476295033/
[23] *Id.*
[24] "Retail Supply Chain at Target Scale" Monday, December 3, 2018 Kaveh Khodjasteh (Target Corporation) https://ima.umn.edu/2018-2019.1/W12.3-7.18/27759
[25] *Id.*
[26] *Id.*

In order to advance solutions to these variables, Target gathers and analyzes data on customers. It was Target that famously used the patterns in its data to predict if customer's were pregnant in order to send coupons aimed at taking advantage of the change in shopping habits that commonly accommodates such a life event.[27]

Target is also in the process of developing a technology that helps with out-of-stock goods. Although the idea has not been implemented in stores, Target plans on using motion detection technology on their existing security cameras to identify when produce is out of stock.[28] Store workers are then notified about the out-of-stock produce via their handheld devices and can know when to run to the backroom to restock the produce.[29]

c. Innovative Technology

Target's strategy involves not just utilizing innovations, but creating and accelerating its own innovations. Target has launched four accelerator programs, including Target Takeoff, Target Incubator, an India-based Target Accelerator Program, as well as the Target Accelerator Program, which "allows [Target] to test a broad set of external innovations that can further differentiate and enhance our guest experience." [30]

In May of 2018, Target announced that it was testing the ability for customers to virtually try un "hundreds of makeup items, including different lip colors, cheek colors and false eyelashes instatement via a new beauty augmented reality experience" on Target.com.[31] The service was also available in select stores using a digital screen in the beauty department.[32]

Target has also provided its customers with computer generated imagery in order to give shoppers an interactive experience. One such technology is an augmented reality feature on Target's mobile website called See It In Your Space ("SIIYS"). SIIYS allows shoppers to see furniture in their rooms before buying it. Specifically, using their smartphones, shoppers can use SIIYS to place real 3-D versions of products within photos of their rooms and adjust them to scale to see how they would look – all before making a purchase.[33] For example, using their mobile device, a shopper picks out a couch that they like. Then, they tap the See It in Your Space button. Next, they upload a picture of their living room. Finally, the app fits the couch to the space provided and allows the

[27] https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html
[28] http://www.startribune.com/target-shows-off-new-tech-it-s-developing/476295033/
[29] *Id.*
[30] https://corporate.target.com/article/2018/12/techstars-fourth-year
[31] https://corporate.target.com/article/2018/05/new-beauty-services
[32] *Id.*
[33] https://corporate.target.com/article/2017/10/see-it-in-your-space

user to rotate and place the couch accordingly. Thus, the shopper does not have to worry about a piece of furniture not fitting the space they bought it for.[34]

d. Results

The Target stock price was up by more than 30% in September 2018.[35] Furthermore, Target reported its best comparable sales growth in 13 years in the second quarter.[36] In its third quarter, comparable sales and traffic increased more than 5% year over year.[37] Online sales grew by 49% over the year ago quarter.[38] Target's digital sales made up 6% of total sales in the third quarter, which is up from 4.2% in 2017.[39] However, shares of Target dropped 15.2% in November,[40] and continued to drop during the month of December.[41] Despite the drop, analysists still insist that investors should not be concerned.[42],[43] With retailers such as Toys R Us failing and Target investing $7 billion into their digital infrastructure, analysists predict that Target will grow earnings 8% per year over the next five years.[44],[45]

b. Companies That Cannot Adapt to Digital World Will Not Exist

i. Blockbuster Case Study

Blockbuster failed to technologically adapt to a digital climate by charging out-of-date fees, delaying by-mail DVD services, and ignoring online streaming. Although Blockbuster had 60,000 employees, 9,000 stores worldwide, a market value of $5 billion and revenues of $5.9 billion, it was only a few years later when these numbers dropped to $120 million in revenue with only 300 stores left in the United States.[46] Today, Blockbuster is a defunct brand with just one U.S. store open in Bend, Oregon.[47] Blockbuster's inability to adopt a change mindset and adapt to the digital world ultimately forced it into bankruptcy and thus pushed it out of existence.

Early Years

The irony behind Blockbuster's inability to adapt to new technological advances is that it began as a revolutionary way to watch movies. In 1985, David Cook founded the

---

[34] *Id.*
[35] https://www.fool.com/investing/2018/12/06/why-target-stock-dropped-15-in-november.aspx
[36] *Id.*
[37] *Id.*
[38] *Id.*
[39] *Id.*
[40] *Id.*
[41] https://www.marketwatch.com/investing/stock/tgt
[42]https://www.fool.com/investing/2018/12/06/why-target-stock-dropped-15-in-november.aspx
[43] https://www.fool.com/investing/2018/11/21/target-and-walmart-stocks-will-bounce-back.aspx
[44] https://www.fool.com/investing/2018/12/06/why-target-stock-dropped-15-in-november.aspx
[45] https://www.fool.com/investing/2018/11/21/target-and-walmart-stocks-will-bounce-back.aspx
[46] https://www.ibtimes.com/sad-end-blockbuster-video-onetime-5-billion-company-being-liquidated-competition-1496962
[47] https://www.adn.com/business-economy/2018/07/12/the-last-two-blockbuster-stores-in-alaska-are-set-to-close/

company when he noticed that movie-rental stores were not specifically catering to their clientele.[48] Cook was able to program computers to keep track of what movies customers were renting. Although most movie-rental stores carried new releases, Cook was able to use the information provided by his computers to determine which older movies customers wanted to rent. This allowed each Blockbuster to optimize which movies it had and cater towards customers in a specific location.[49] Only two years later, Cook was able to sell the company to Harry Wayne Huizenga for $18.4 million. After opening almost 3,000 locations and generating nearly half a billion dollars in annual revenue, Huizenga sold the Blockbuster brand to Viacom for $8.4 billion dollars.[50]

Netflix: Subscription Fees, Late Fees, and By-Mail DVDs

In 1997, Reed Hastings and Marc Randolph created Netflix after supposedly obtaining a $40 late fee from Blockbuster for failing to return *Apollo 13* on time.[51] Unlike Blockbuster, Netflix charged a monthly subscription fee that allowed consumers to order DVDs online, receive them in the mail, and keep them as long as they wanted without late fees.[52] However, Blockbuster continued to charge late fees on top of charging a monthly fee until the end of 2004.[53] Furthermore, in 2000, Reed Hastings approached Blockbuster to buy Netflix for $50 million, an offer in which Blockbuster declined.[54] Moreover, Blockbuster did not begin a mail-subscription service until 2004; almost seven years after the launch of Netflix.[55]

Although Blockbuster launched its mail-subscription service in 2004, it did not take off until late 2006, when it upgraded the service to "Blockbuster Total Access."[56] With Blockbuster Total Access, customers could receive movies via mail and have the option to bring them back to any store in the country and exchange them for new movies for free. However, every time a customer exchanged one of their movies in stores, it costed Blockbuster $2, a cost that it hoped to recoup through new subscribers. However, it was unable to regain its losses.[57]

During this period of time, Hastings met with then-Blockbuster CEO John Antioco so that Netflix could buy Blockbuster's online branch and market.[58] However, investor Carl Icahn was opposed to the idea and forced Antioco out of his position as CEO, thus

---

[48] http://content.time.com/time/magazine/article/0,9171,2022624,00.html
[49] *Id.*
[50] *Id.*
[51] http://www.businesspundit.com/10-businesses-that-failed-to-adapt/2/
[52] https://www.wired.com/2002/12/netflix-6/
[53]https://trace.tennessee.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1010&context=utk_studlawbankruptcy&gt
[54] https://www.businessinsider.com/blockbuster-ceo-passed-up-chance-to-buy-netflix-for-50-million-2015-7
[55]https://trace.tennessee.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1010&context=utk_studlawbankruptcy&gt
[56] https://www.npr.org/templates/story/story.php?storyId=9151791
[57] https://www.fool.com/investing/general/2013/11/14/how-blockbuster-almost-beat-netfilx.aspx
[58] *Id.*

ending the potential deal between the two companies.[59] Subsequently, the price of Blockbuster Access was raised and the free in-store exchanges were stopped.[60]

Online Streaming

In 2007, Netflix launched its online streaming service.[61] Online streaming allowed customers to watch videos on demand via the internet. Although this is what Netflix is known best for today, the online streaming market was "microscopic" at the time.[62] Thus, Netflix looked to where technology was headed in order to adapt to a rapidly growing digital market. A year later, Hulu launched a competing service, allowing customers to watch their favorite shows via online streaming.[63] In 2008, Blockbuster bought MovieLink, a company backed by five major movie studios that provided digital movie downloads.[64] This gave Blockbuster the chance to buy the exclusive digital rights to movies on an exclusive basis that would have prevented Netflix from streaming those movies.[65] However, Blockbuster declined to purchase the rights and instead focused on setting up locations called "Blockbuster Express" to compete with Redbox, a company that rents movies out of a vending machine-like kiosk.[66] In fact, the Blockbuster CEO was quoted stating, "Netflix *[is not]* even on the radar screen in terms of competition. It's more Wal-Mart and Apple."[67] Once again, Blockbuster strayed from adopting new technology in order to adapt to a digital world.

End Times

The increasing number of competitors that provided immediate access to movies ultimately replaced the request for the rental and sale of physical DVDs.[68] Between 2008 and 2010, Blockbuster experienced rapid decline, closing over 1000 stores.[69] On September 23, 2010, Blockbuster filed for Chapter 11 bankruptcy.[70] Subsequently, Blockbuster was delisted from the New York Stock Exchange and Dish Network bought its remaining stores.[71] Since the purchase, all but one Blockbuster in the U.S. has been sold.

---

[59] *Id.*
[60] *Id.*
[61] https://www.nytimes.com/2007/01/16/technology/16netflix.html
[62] *Id.*
[63] https://www.hulu.com/press/about/
[64] https://www.dmagazine.com/business-economy/2018/04/former-ceo-jim-keyes-why-blockbuster-really-died-and-what-we-can-learn-from-it/
[65] *Id.*
[66] *Id.*
[67] https://www.fool.com/investing/general/2008/12/10/blockbuster-ceo-has-answers.aspx
[68]https://trace.tennessee.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1010&context=utk_studlawbankruptcy&gt
[69] https://www.chicagotribune.com/entertainment/ct-xpm-2010-10-20-ct-live-1020-video-stores-borrelli-20101020-story.html
[70] http://www.pacermonitor.com/view/PXDYCPY/Blockbuster_Inc.__nysbke-10-14997__0001.0.pdf
[71]https://trace.tennessee.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1010&context=utk_studlawbankruptcy&gt

Blockbuster's failure to adapt to a digital world ultimately destroyed its business. Its late-to-the-game elimination of fees and offering of by-mail DVDs, and online services could not match the fast paced innovation of its main competitor, Netflix. It is companies like Blockbuster that remind today's businesses that technological adaptation is absolutely necessary to succeed in today's market.

c. Franchisee Participation and Communication

While numerous changes, technology and otherwise, are foreseeable within a franchise system, franchisors will always face some type of resistance from franchisees. The best way to ensure success of the proposed technology change is for the franchisor to work with franchisees to identify, develop, communicate and implement the system-wide addition or modification.

Successful communication to the franchise system regarding the "why" we are changing will influence the adoption and engagement of the change throughout the franchise system. There are two basic scenarios in which an organization can communicate the reason behind change.

The first scenario is when the need for change was determined by the franchisor without any franchisee consultation. This situation can prove to be more difficult for the franchisor to communicate the technology change as the franchisees' first introduction to the reasons behind the change are simultaneous with the new technology solution itself. By combining the "why" and the solution in the same communication the organization has removed the franchise system from the discussion and ultimately does not allow the franchisees the time to process the need for change which may affect adoptability of the new technology.

The second scenario in which the need for change can be communicated to the franchise system includes franchisee participation in defining the need for change and/or reviewing any possible technology solutions. When a franchisor seeks franchisee involvement, it allows experienced franchisees to contribute their relatable need for change, which adds to the franchisee support and advocacy for the technology change to the entire franchise system. While system-wide participation may not be reasonable in all situations, every effort should be made to involve some sampling of franchisees.

i. Why is the Franchise System Changing?

A crucial part of the communication, roll-out and ultimate success or failure of a technology change rests upon the reason why the change is occurring. Is it to increase sales, improve efficiency, legally required (PCI compliance), garner a competitive advantage or decrease costs or processes? Any of those reasons would be justification for a system-wide technology change, however, if the "why" is not communicated in a transparent manner based on sound business research and / or trials, a franchisor can be faced with low system support and implementation.

Business plans/cases are required for several different activities such as obtaining a loan, purchasing a franchise and just understanding your business with more clarity. Business cases also provide franchisors an opportunity to demonstrate the need for the technology change and the return on investment the franchisee should achieve. A business case built on diligent research conducted on its customers, demographics, competitors, and industry as a whole will help the franchisor identify the risks and address those in advance of any franchisees' assumptions and/or misperceptions.[72] A sound business case has the ability to garner support for the change throughout the system, strengthen the franchisor-franchisee relationship and can limit the risk of any potential litigation.

A franchisor can build its business case for the technology change in several different ways, but two of the more influential methods that demonstrate the value of the change and return on investment are based on either the franchisor's company store pilot or an early adopter program.

If a franchisor has corporately owned units they should consider piloting the change in their units to understand how the change affects the daily activities, make any modifications or improvements, observe any impacts and thoroughly document the results for their business case.[73] Piloting at corporately owned locations also demonstrates a franchisor's good faith in implementing the change throughout the system, as they are in essence, "buying what they are selling."

An early adopter program can work in conjunction with a franchisor's company store pilot or can be utilized on its own merit if a franchisor does not have corporately owned units. The early adopter program is not only instrumental in working out the kinks of a new technology, but also in obtaining support throughout the franchise system for a change that may favor the franchisor over the franchisees or if the franchisor may not have express authority to require the change.[74] The success or failure of an early adopter program may be directly impacted by the franchisees that the franchisor selects to participate in the program. The franchisor will need to ensure there is a wide variety of franchisees in the early adopter pool, to dispel any perceptions that the results from the early adopter program is bias.[75] The ultimate goal of both a company store pilot and early adopter program is to be transparent with the results of the technology change while demonstrating the value of the change, the true costs incurred during the implementation and the ease or difficulty with the implementation and process change.

---

[72]Chris Dull, Clint Ehlers, Andraya Frith, and Max Staplin, "Ch-ch-ch-ch-changes: Implementing System Changes, Upgrades and New Directions Under Existing Franchise Agreements" (Paper delivered at the IFA Legal Symposium, Washington, D.C., May 7-9, 2017) at 16.
[73] *Id.* at 17.
[74] Jonathan Koudelka, Gillian Scott, Brenda Trickey, and Alexander Tuneski, "Winds of Change-Tried Techniques For Effectively Managing Risk When Implementing System-Wide Changes" (Paper delivered at the IFA Legal Symposium, Washington, D.C., May 15-16, 2016) at 40.
[75] *Id*.

ii. Communicating the "How" is the Franchise System Changing?

Once a franchisor has identified and communicated the need for change to either address an issue or to enable the franchise system a competitive advantage, the franchisor then needs to communicate how the change is going to be implemented and the effect on the individual franchisees.

While the "how" of the technology change may be the simplest of the communication processes, it also may be the most vital to the success of the change implementation. If franchisees do not understand how to implement the change, the timing of such change or how it will ultimately affect their daily business and processes, franchisee adoption and buy-in will be halted.

The communication that explains to the franchisees how they will implement the change needs to be concise and simple. While franchisees may have a desire and demand to know the exact timeline for all tasks of implementation, it is advisable for the franchisor to allow for fluctuations in the timing for any unforeseen issues. The communication to the franchise system of an issue and or need, coupled with the change solution generates excitement and expectations. The technology change and its implementation process can become negative quickly when timelines and expectations are missed, whether in reality or just in perception.

iii. Utilizing Franchisee Advisory Councils and Independent Franchisee Associations

A vital component in both the proposed change and the promotion of that change to the franchise system is the Franchisee Advisory Councils (FAC), or in some systems, independent franchisee associations.[76]

FACs and independent franchisee associations are usually compromised of experienced franchisee leaders, whom will provide thoughtful feedback, suggestions, aid in the communication and implementation process, and possibly become early adopters of the technology change. Working with a FAC or association throughout the technology change process also enables the franchisor to understand and resolve the contentious issues that they may face during the franchise system-wide implementation.[77]

A franchisor's relationship with their FAC or franchisee association is a critical component of the change process. Ideally, the FAC or association, become the advocate of the change to the franchise system, in essence "selling" the change to their franchisee counterparts on the franchisor's behalf.[78] If a franchisor has a positive relationship with their FAC or franchisee association and can gander their support of the technology change, the likelihood of a successful change implementation is great. However, if the Franchisor has a relationship with the FAC, franchisee association or the franchise

[76] Dull, *supra* note 72 at 18.
[77] *Id.*
[78] *Id.*

system as whole, which involves a history of poor communication and lack of trust, the technology change will likely be met with objection and low adoptability.

iv. Sample Outline of Communication Process

- Determine the high-level issue or need for change based on competitive research or franchisee feedback;
- Identify a group of influential franchisee leaders, FAC or independent franchisee association, to discuss the need for change and define the possible resolutions;
- Once the technology solution has been determined, the franchisor and the FAC / association should establish a communication plan to the franchise system in unison to gain gander more engagement and "buy-in" throughout the franchise system;
- The communication structure should include a true feature / benefit structure so that the "why", "what" and "how" are easily understandable by the masses;
    - Need for change – should include the issue or competitive advantage that the change is addressing as well as how it affects the franchisee;
    - How the issue identified is currently affecting the franchisee or how the change will affect the franchisee;
    - The solution being proposed and how it will improve the issue or add a competitive advantage for the franchisee;
    - A simplistic outline of the steps or tasks required of the franchisee to implement the change and an estimation of the timeline of implementation; and
    - Any follow-up process and expectations once the change has been fully deployed and implemented.

II. Implementing Technology System Changes Under Existing Franchise Agreements

The evolution of a franchise system in the current technology driven economy is inevitable. If a franchisor does not identify the need for change, communicate and obtain franchisee buy-in and adoption then their brands will become as obsolete as Blockbuster. In the event a franchisor has attempted to not only communicate the why, how and when of the change and seek franchisee feedback, they may still face franchisee opposition. However, the franchisor might be able to force the system-wide change through the franchise agreement, with or without franchisee support.

a. Good Faith and Fair Dealing

Good faith and fair dealing have significant impact in a franchise relationship not only through specific provisions of franchise agreements, but also through common law's

precedent to imply the duty of good faith on all parties to a franchise agreement.[79] Good faith and fair dealing are not terms that overwrite contractual provisions, but instead dictates the manner in which a contractual provision is enforced or how a franchisor utilizes its contractual discretion.[80]

The scope and applicability of the duty of good faith is continually evolving in the arena of contract performance and a franchisor's use of their discretion, Scott et al. outlined four guiding principles the North American jurisprudence utilizes in assessing a party's compliance with the duty:

- Franchisor's motives matter;
- Contractual discretion must be exercised reasonably;
- Courts will defer to the franchisor's business judgment; and
- A franchisor's engagement in meaningful dialogue with the franchisees regarding the change will be beneficial in defending against allegations for the breach of good faith and fair dealing.[81]

As discussed above, the best way for a franchisor to communicate the change and also to demonstrate its good faith is to develop a sound business case that justifies and supports the franchisor's discretion to implement the system-wide change.[82]

b. Franchise Agreement

The basis of a franchise relationship is the franchise agreement and in order to implement a system-wide technology change a franchisor should first look to its franchise agreements to confirm it has the contractual authority to mandate such a change.[83] Undeniably, "the express terms of the franchise agreement will [often] be dispositive of any franchisee action with respect to system-wide change."[84]

There is a two-prong strategy in drafting a franchise agreement that is not change adverse, but change embracing:

1. General terms that build in flexibility of the franchise relationship; and
2. Specific terms that address an anticipated or foreseeable change in the future.[85]

By incorporating broad general contract clauses in the franchise agreements, franchisors enable themselves to implement system-wide changes without the need for negotiations and amendments. These types of clauses usually include the typical

[79] Dull, *supra* note 72 at 14.
[80] *Id.*
[81] Scott, *supra* note 74 at 29-30.
[82] Dull, *supra* note 72 at 15.
[83] *Id.* at 4.
[84] Scott, *supra* note 74 at 20.
[85] Dull, *supra* note 72 at 5.

language of "as the Franchisor may designate or approve from time to time." By including this contractual authority in the franchise agreement, the franchisor has granted itself the ability to change the technology used by the franchise system without the need for manual updates, franchise agreement amendments, or incentives to sign a new franchise agreement.

While general contractual clauses are necessary for the foundation of change, specific clauses are important when a change is foreseeable, such as changing required software, or approved suppliers.[86] If an area of technology change is addressed in a specific clause, courts will apply the specific clause instead of the general clause containing a reservation of rights.

c. Operations Manual

Franchisors can also utilize their operations manual to implement a system-wide change. Franchising in its basic terms is where a franchisor licenses their trademarks and their "system" to a franchisee. In order to maintain consistency across the brand and its standards most franchisors incorporate the contractual requirement to follow their operations manual that the franchisor has the ability to change in its sole discretion from time to time.

While amending a franchise agreement requires both parties to agree to the modification, the franchisor can update and modify the manual in its sole discretion. Franchisors should be conscious of the appearance of unilateral modification when making significant changes to the system or changes that require the franchisee invest a significant amount. To ensure the franchisor-franchisee relationship is not irreparably harmed and to lower the franchisor's legal risk, system-wide changes implemented through modifying the operations manual should be limited to only those changes that were reasonably foreseeable at the time of the franchise agreement was executed.[87]

d. Implementing a Technology Fee

Franchisors and franchisees should understand the difference between a software fee, which a franchisee pays for access to a certain software platform and a technology fund fee. A technology fund fee operates in the same manner and concept as an advertising fund fee. A franchisee pays a set amount, usually a percentage of gross revenues, into a fund that the franchisor utilizes for the benefit of the franchise system by investing in new technology opportunities to create a competitive advantage.[88]

Once a franchisor has determined that there is a need for a technology fund for the franchise system, the implementation of the technology fund fee begins with amending the franchise disclosure document and correlated franchise agreement. While

---

[86] *Id.* at 8
[87] Scott, *supra* note 74 at 7.
[88] See Appendix A for sample Technology Fund provisions.

updating the franchise disclosure document enables the franchisor to collect technology fund fees under future franchise agreements, simply amending the current franchise agreement does not apply the technology fund fee retroactively to existing franchise agreements.

Some franchisors will choose to not retroactively apply the technology fund fee to existing franchisees and will instead opt to have the fee applicable upon a new franchise agreement being signed, whether that's through a new franchise sale, an acquisition of an existing franchise, a franchisee's territory expansion or a franchisee's renewal of their franchise agreement. This approach allows for existing franchisees to appreciate the need for a technology fund and the competitive advantage that it will create for the franchise system as whole, prior to the fee being applicable to their franchise.

If the franchisor instead desires the technology fund fee be applicable to everyone right out of the gate, they may need to consider incentives to the existing franchisees to either amend their current agreements or sign a new franchise agreement. When a franchisor does not have the contractual authority to force the fee on existing franchisees, incentives may garner franchisee support for the technology fund fee. Incentives may also be the key for implementation or "buy-in" when franchisees perceive the fee favors the franchisor or where the franchisor faces tremendous pushback.[89]

Some sample incentives include but are not limited to:

- Short-term royalty reductions;
- Deferring the fee implementation for a period of time;
- Discounting or waiving early renewal fees;
- Increasing the term of the franchise agreement;

As discussed, although the franchisor may still have the ability to force the system-wide change through the franchise agreement, it may not be the preferred method for a franchisor, as exercising this authority without franchisee support and collaboration could be detrimental to the franchise relationships and network in the long-term.

III. Evaluating Different Technologies and Innovative Ways to Deliver Products and Services within a Franchise System

There is no doubt that innovation and technology have disrupted many industries. Whether you are a small business owner or a large franchise system, businesses must constantly evolve or be left behind. And innovation is not a one-time-and-done transaction. Rather, businesses must constantly be evaluating what is the next "disrupter" and developing strategies to stay ahead. Franchisors and franchisees alike must keep innovating or risk sudden death.

[89] Dull, *supra* note 72 at 20.

One franchisor that has embraced the concept of innovation through technology is Domino's Pizza, which was recently named "2018 Tech Accelerator of the Year" by *Restaurant Business*.[90] Domino's has hailed itself as "a tech company that happens to serve food."[91] This didn't happen overnight. Domino's Chief Digital Officer stated, "we used to be a pizza company that sells online, and we needed to become an e-commerce company that sells pizza."[92] In April 2009, Domino's stock price was less than $10. Ten years later, its stock price is nearly $260. In 2009, Domino's had global system wide sales of $3.1 billion. In 2018, Domino's reported global system wide sales of $13.5 billion.

Some of the many innovations implemented by Domino's include on-line pizza tracking and ordering by mobile device, tweet, Facebook messenger, or voice commands via Alexa, Echo and Google Home. Customers can even order by using pizza emojis 😋. Domino's introduced delivery to Hotspots®, so customers can have pizza delivered to nearby locations that do not have a physical address and has an on-line pizza wedding registry in the event customers want to send the engaged couple a gift for the "2 a.m. Bachelor Party Feast", "The Wedding Night" or "Post-Honeymoon Adjustment to Real Life". But Domino's innovation doesn't stop there – Domino's is continuing to evaluate new technologies and ways to deliver its pizza, including use of artificial intelligence and automated delivery by drones or self-driving vehicles.

"Embracing innovation within a franchise environment – from the corporate support teams to the franchise owners – is critical for positive evolution and long-term success."[93] So what are the challenges in implementing new technologies and innovative ways to deliver products and services within a franchise system? How do these changes affect the franchisees? And what are some strategies for overcoming those challenges?

a. Challenges to Consider

Whether introducing a new software system, a mobile ordering platform, online delivery of products and services, or drone delivery, there are a number of challenges a franchisor should consider. These challenges will require careful evaluation of the legal rights and obligations of the parties under the terms of the franchise agreement, as well as various other business considerations.

i. The Franchise Agreement

---

[90] Domino's Named 2018 Tech Accelerator of the year, *Restaurant Business* (October 2, 2018), online: https://www.restaurantbusinessonline.com/technology/dominos-2018-tech-accelerator-year.
[91] *Id.*
[92] How Domino's is using tech to woo Millenials and beat rival Pizza Hut, *Detroit Free Press* (March 6, 2018), online: https://www.usatoday.com/story/money/business/2018/03/06/how-dominos-using-tech-woo-millennials-and-beat-rival-pizza-hut/399837002/.
[93] Top Five Strategies for Embracing Innovation in the Franchise System, *Forbes* (May 4, 2018), online: https://www.forbes.com/sites/forbescommunicationscouncil/2018/05/04/top-five-strategies-for-embracing-innovation-in-the-franchise-system/#4847740b600c.

When developing new and innovative ways to deliver products and services ("alternative distribution channels"), the applicable franchise agreements should be reviewed to determine any potential challenges. Some issues to be reviewed include:

- Does the alternative distribution channel affect the franchisee's territory?

- Does the franchisee have the right or obligation under the franchise agreement to participate in the alternative distribution channel?

- What are the rights and obligations in relation to royalties, fees and costs?

With implementation of alternative channels for delivery of products and services, the franchisor must consider any territory limitation in the franchise agreement. The franchise agreement may contain an exclusive territory provision, but what does that provide or restrict? Does the franchise have the right merely to operate at a designated location or does the franchisee have rights to customers that reside in the territory? Does the franchise agreement have a broad reservation of rights provision allowing the franchisor to exclusively conduct the alternative distribution channel?

Franchise agreements have varying rights and obligations. For illustration, at one end of the spectrum, a franchise agreement for a learning center provides that the franchisee does not have an exclusive territory and that the franchisor can serve students online, can sell and distribute workbooks online, and can license other schools at any location to use the proprietary methods of the learning center. Another franchise agreement for an electronics repair franchise provides that the franchisor has the exclusive right to market repair services online, including remote support and assistance and mail in repairs. However, adopting a middle approach, the franchise agreement states that the franchisor may refer online customers to franchisee at its discretion and may charge an administrative fee for any referred clients in addition to regular royalties.

On the other end of the spectrum, some franchisors require franchisees to participate in e-commerce channels. A franchise agreement for a small electronics retail chain provides that, for internet purchases within a certain distance from the franchise store location, website transactions are assigned to that franchisee to fulfill and the franchisee pays the standard royalty rate plus administrative fees and expenses related to the e-commerce program. Franchisees are also required to participate in a separate omni-channel program for e-commerce transactions to larger retail, national account and business customers, and must pay a $10,000 annual access fee as well as related administrative fees for monthly software support, and various other program and maintenance fees.

In addition to a careful review of existing franchise agreements to determine the rights and obligations as they currently exist, as franchisors update their franchise agreements, they must consider future innovation and the respective parties' rights and obligations.

ii. Other Business Considerations

In addition to the rights and obligations under the franchise agreements, there are other business considerations, including:

- Whether franchisees will be allowed to participate?
- Whether participation will be optional or mandatory?
- What are the requirements for participation?
- Whether franchisees will be resistant to the change?
- Whether there will be added cost to franchisees?
- What is the timing of implementation?

Franchisors must balance the benefits and disadvantages of franchise participation in any new alternative distribution channel, as well as whether any participation will be on an optional or mandatory basis. Factors to consider (aside from the requirements under the franchise agreement) may include: the need for franchise participation to meet customer demand; financial cost/revenue implications; the technical ability of the franchisees; the need for franchisee input and feedback; and the potential impact on the overall franchisor/franchisee relationship. If a new channel is in its infancy and customer demand and profitability are not well known, the franchisor may consider an initial pilot program without franchise participation at the preliminary stages so that the franchisor can more readily adapt and adjust as needed depending on results. Alternatively, it may be helpful to have a select group of franchisees participate in a pilot program to gain additional learnings from participating franchisees in relation to the franchisees' cost and operating model and gain insight on future implementation in other franchise locations. Allowing franchisees to participate, either on a pilot or limited basis, may also alleviate franchisee concerns that the franchisor is attempting to cannibalize their business and divert revenue from franchisees.

The franchisor should also consider any requirements for franchise participation. These may include service level agreements, additional required training, process or operational requirements, and required purchase of additional supplies and equipment. If not otherwise provided in the franchise agreement, a separate participation agreement or addendum to specify the specific program requirements, franchisee costs and applicable royalty payments may be needed.

Franchisee resistance should also be taken into account. For established franchise systems, some franchisees may not see the benefits of new technology or the benefit of innovative new ways to delivery products and services. This resistance may be amplified if franchisees will be required to incur significant additional costs. Careful consideration

must be given to whether franchisees see the need for change and the financial impact to the franchisees' business.

In addition, franchisors must evaluate the timing of the implementation and whether any new program will be rolled out all at once or in phases. This may be dependent on some of the other issues noted above, such as customer demand, the need for additional testing on costs, revenue and profitability, and the impact of these costs on the franchisees. A more phased in approach may be more advisable the greater the amount of change and cost to the franchisees.

b. How Do Technology Changes/Innovation Affect Franchisees

A key component to implementation of new technology or alternative distribution channels is to understand how it will affect the franchisees. Technology changes should be evaluated in terms of creating efficiency for franchisees and giving them additional tools and resources to increase their revenue and profitability. "Technology should not be a burden to franchisees; it should free up more of their time to focus on the guest and initiatives that will spur growth."[94]

However, with changes comes change management. Franchisees and their staff may need additional training, resulting in more time and costs during the implementation. This may lead to lower profitability, which may be short-term or long-term depending on the significance of the change. For example, rolling out a completely new software system may require a significant amount of training and time to work out any unidentified issues within the system.

Alternatively, if franchisees are not eligible to participate in a new, alternative distribution channel, franchisees may be affected by a loss of customers and revenue due to customer migration – such as where brick-and-mortar retail customers migrate to on-line purchases. It is therefore critically important that franchisors develop appropriate strategies to overcome these challenges and ensure that franchisees understand the need for the change and are advocates to ensure the success of the brand.

c. Strategies for Overcoming Challenges

There are a number of strategies to ease any challenges involved in implementing new technologies or alternative ways to deliver products and services. One important strategy is to communicate with franchisees regarding the need for change. As demonstrated by Blockbuster, a brand that does not continue to innovate, may no longer exist. It is important that franchisees understand that changes are necessary to provide a competitive advantage and to ensure continued success of the brand. Success of the brand is critical to the franchisees' success.

---

[94] How Restaurant Technology is Evolving in the Franchise Industry (July 27, 2018), online: https://www.smoothiekingfranchise.com/franchise-resources/how-restaurant-technology-is-evolving-in-the-franchise-industry/.

Franchisors should also collaborate with franchisees and involve them in the innovation process. “By embracing the franchisees’ ideas and backing them up with the right resources, organizations will know they are working on the right things and introducing changes that franchise owners will be excited to adopt.”[95] Franchisees have valuable insights and are more likely to adopt changes that they were a part of or in which they had some involvement. If a franchise advisory council exists, work with the council to get franchise feedback and develop a strategy for implementation based on the council’s feedback and guidance.

Consideration should be given to potential incentives or benefits to franchisees to gain greater adoption of the change. These may include royalty or cost reductions if certain targets or milestones are achieved. Another strategy is to educate franchisees on cost savings that may result from greater efficiencies, as well as increased profitability due to greater customer satisfaction.

To the extent possible, establish transparency with the franchisees. “Encouraging innovation with a high degree of transparency is important because it allows the organization as a whole to measure results, understand scalability, and quickly share what is working with the remainder of the system.”[96] Share results with franchisees so that they understand both the positives and the negatives and can be part of the process to adjust and fix what is not working. Innovation can be disruptive and may lead to failure; learning and adapting is necessary. If franchisees are part of the learning process, they are more likely to embrace change.

III. Negotiating and Administering Complex Technology Vendor Transactions

Once a franchisor determines to move forward with implementing new technology into its franchise system, the franchisor will need to negotiate a technology vendor agreement. Two areas a franchisor should focus on in the technology vendor agreement is allocating risk for data breach and service level requirements.

a. Allocating Risk for Data Breach and other Privacy Issues

Allocating risk for data breach and managing other privacy issues in vendor relationships is subject to heavy debate. On one hand, sector specific laws such as the Health Insurance Portability and Accountability Act (“HIPAA”) and the Gramm-Leach Bliley Act typically govern the steps organizations need to take to protect data with vendors. For example, HIPAA regulates the standards that must be in place between a “covered entity” and a “business associate.” On the other hand, applying traditional tort

[95] *Top Five Strategies*, *supra* note 93.
[96] *Id.*

law and contract law to data privacy issues has proved to be inconsistent and difficult for courts to apply because of the complexity of technology. To muddy the waters even more, agencies such as the Federal Trade Commission ("FTC") and the U.S. Securities and Exchange Commission ("SEC") have large discretion when deciding how and when they enforce privacy issues. In turn, organizations have great difficulty knowing how to allocate risk when they enter into vendor relationships.

Despite the confusion, there are steps that organizations can take to allocate risk in vendor relationships. The following explores two current trends for managing privacy issues when dealing with vendors: establishing a data and privacy vendor management process and contractually allocating risk with standard contractual provisions.

i. Establishing a Privacy and Data Security Vendor Management Process

Organizations should consider establishing a formal privacy and data security vendor management process that, at a minimum, consists of: (i) performing pre-engagement vendor due diligence; (ii) developing and implementing standard contract terms that support the organization's privacy and information security programs; and (iii) engaging in periodic reviews and ongoing oversight of the vendor throughout the contract term.[97]

1. Pre-Engagement Due Diligence

Pre-engagement due diligence is intended to determine whether vendors have appropriate privacy and information security programs and procedures in place before an organization allows a vendor to access its systems or data. Organizations should consider creating and consistently using a standard privacy and data security vendor assessment questionnaire. Some key points to address in vendor due diligence questionnaires[98] include: how the vendor complies with any applicable laws and regulations, the vendor's current data privacy and information security policies and procedures, any past security incidents, insurance coverages and any regulatory or enforcement actions.[99]

2. Contract Drafting and Negotiating Strategies

Organizations should develop and impose standard privacy and data security contract terms and/or a security addendum[100] to ensure that vendors protect the organization's data and systems in a manner that meets or exceeds the organization's own practices and complies with applicable laws, regulations, and industry standards.

---

[97] Matthew Karlyn, Foley & Lardner, (Strafford Webinar Delivered January 16, 2019) *Integrating Information Security into the Supplier Contracting Process*

[98] See Appendix B for Sample Vendor Vetting Questionnaire

[99] Karlyn, *supra* note 97.

[100] See Appendix C for template Security Addendum

Vendors often seek to use their own privacy and data security terms and conditions. These vendor-friendly provisions may not meet the organization's requirements. However, even if business circumstances dictate using a vendor's agreement, by developing its own standard terms, an organization can better assess and manage the risks of using vendor-supplied terms.

a. Standard privacy and data security contract terms

Notice and Cooperation Clauses

Vendor contracts should define "cybersecurity event" or "breach of security" as broadly as possible and should also include definitions for "confidential information" that include personally identifiable information and protected health information of customers and employees, as well as any information that will be shared between the organization and the vendor.[101] The notice clause should contain specific language including a time period for reporting and a description of to whom the notice should be directed, and be tied back to the defined term "cyber-security event" or "breach of security."[102]

The cooperation clause should state that the vendor will cooperate with the organization during any investigation necessary after the discovery of a cybersecurity event.[103] The cooperating clause is an important tool to make sure the vendor will help facilitate such investigations.[104]

Cyber Liability Insurance and Indemnification

Vendor contracts should include clauses that reduce the risk of financial burden in the event that a vendor causes a cybersecurity incident.[105] Thus, a provision should be added that requests insurance information for stand-alone cyber liability coverage, including the limits available, retention levels and whether the policy form grants coverage for the organization.[106] In the event that the vendor does carry stand-alone cyber liability coverage, organizations should add a provision specific to cybersecurity events that requires that the vendor indemnify costs related to notification, legal fees, judgments, settlements, forensic experts and public relations efforts.[107] Organizations should be careful to exclude cybersecurity provisions from limit of liability sections that may govern more general indemnification provisions.[108] Typically, such provisions will be capped at a low dollar amount or at the monthly fee the organization is paying the vendor.[109]

---

[101] http://www.rmmagazine.com/2017/05/01/using-contracts-to-curb-cyberrisks/
[102] *Id.*
[103] *Id.*
[104] *Id*.
[105] *Id.*
[106] *Id.*
[107] *Id.*
[108] *Id.*
[109] *Id*.

Minimum Standard of Care

Vendor contracts should define and obligate the vendor to meet a minimum standard of care for privacy and data security, which may exceed or be more prescriptive than applicable laws and industry standards to meet the organization's needs.[110] The minimum standard of care is typically defined by combining explicitly defined safeguards; specific industry standards, such as the National Institute of Standards and Technology ("NIST") Cybersecurity Framework or the Center for Internet Security ("CIS") Critical Security Controls; the organization's privacy and information security policies as provided by the vendor; and applicable laws and regulations.[111]

Third Parties

Vendor contracts should prohibit the vendor from disclosing the organization's data to third parties except as specifically authorized by the organization, such as to subcontractors or the vendor's legal counsel or other advisors.[112] Disclosure prohibitions should also address how to handle data requests from government authorities.[113] Further, vendor contracts should require the vendor to pass the same privacy and data security obligations through to its subcontractors or other service providers and engage in the management and oversight necessary to ensure compliance by these third parties.[114]

Audit

Vendor contracts should provide the organization with rights to audit or otherwise assess and review the vendor's privacy and data security practices.[115] Common methods include direct vendor audits or assessments performed by the organization or its contractors, self-assessment performed by the vendor at minimum intervals, independent third party audits, assessments, or certifications, or a combination of methods based on timing and risk.[116] Audits should take place during pre-engagement due diligence review and periodically throughout the relationship.[117]

Other General Provisions

Vendor contracts should permit the vendor to access the organization's IT systems and use its data only to the extent required to perform the agreed-upon services, unless the organization specifically grants authorization, such as to allow the vendor to use its data for research or development purposes.[118] Further, the vendor contract should require

---

[110] *Managing Privacy and Data Security Risks in Vendor Relationships,* Practice Note, Practical Law Intellectual Property & Technology, Westlaw, USA (National/Federal)
[111] *Id.*
[112] *Id.*
[113] *Id*.
[114] *Id.*
[115] *Id.*
[116] *Id.*
[117] *Id.*
[118] *Id.*

the vendor to return or destroy, at the organization's request, all copies of the organization's data upon termination of the agreement.[119]

3. Ongoing Oversight and Enforcement

As part of the vendor management process, organizations should establish a cadence of periodic review of vendors to ensure vendors are performing their contractual obligations with respect to data privacy and security. Establishing an ongoing vendor oversight process also assists in identifying issues early before potentially serious consequences could arise. Ongoing vendor oversight processes also may help demonstrate in litigation or regulatory enforcement actions that an organization acted reasonably under the circumstances.

If a vendor has access to particularly sensitive data, such as your customers' protected health information, organizations may consider requiring vendors to provide independent third-party assessments, audits, or certifications during pre-engagement due diligence and on an ongoing basis throughout the contract term. Organizations may also choose to conduct themselves or require potential vendors to conduct specific technical risk assessments such as penetration tests or vulnerability scans.

b. Service Level Requirements

The purpose of service level requirements are to ensure the customer can rely on the availability of the services, provide appropriate remedies for service interruptions and provide incentive for the vendor to remedy service interruptions in a timely manner.[120]

i. Common contractual provisions

Service Availability

Service interruptions may seriously affect the business operations of perhaps both the franchisor and franchisees by denying access to critical software systems and customer data. Technology agreements should include service availability provisions that align with the business needs of the franchise system. General service availability is typically provided as the uptime percentage or the percentage of defined time period that the service will be available and operational for the customer to use.[121] Uptime percentages typically range from 99.5% to 100%.[122] Appropriate uptime percentages may vary depending on the nature of the services. If the services are mission critical to your business, consider asking for a closer to 100% uptime percentage.

---

[119] *Id*.
[120] *Software as a Service (SaaS) Agreements,* Practice Note, Practical Law Intellectual Property & Technology, Westlaw, USA (National/Federal)
[121] *Id.*
[122] *Id.*

Scheduled Downtime

Technology vendors typically reserve the right to schedule downtime to conduct routine maintenance.[123] However, if the service is critical to your business, consider negotiating that the vendor maintain redundant service systems.[124] Another option, is to allow for scheduled downtime but only with advance written notice of the downtime and restrict the permissible dates and times that meet the customer's business operations.[125] Vendors will typically exclude scheduled downtime from the calculation of service unavailability. Customers should consider negotiating scheduled downtime to be treated as any other service outage when calculating uptime percentages.[126]

Service Support

Support service level requirements obligate the vendor to time based performance standards concerning service errors, response time and resolution time.[127] Response time is the time from which the customer notifies the vendor of a service interruption or error and requests correction to when the vendor confirms receipt of the request and begins to resolve the issue.[128] Resolution time is the period of time from when the customer requests correction of an issue to when the vendor permanently resolves the issue with a fix or a work around.[129] Resolution time is the more critical of the two standards for the customer.[130] The customer should therefore ensure the contract provides that the vendor is required to fully correct errors and not just respond to service errors the customer brings to the vendor's attention.[131] The customer should also consider whether after business hours support is necessary and address that in the contract if needed.[132]

ii. Remedies for Failure to Satisfy Service Level Requirements

The two most common remedies for failure to satisfy service level requirements are service credits and termination of the agreement. Service credits are a current standard in service level agreements while termination is not as common. However, it is important for customers to address both in their vendor agreements.

Service Credits

It is now a standard in service level agreements to include a service credit mechanism, where the customer receives a credit if the vendor performance does not

[123] *Id.*
[124] *Id.*
[125] *Id.*
[126] *Id.*
[127] *Id.*
[128] *Id.*
[129] *Id.*
[130] *Id.*
[131] *Id.*
[132] *Id.*

meet the contracted performance standard for a service level.[133] Service credits are pre-specified financial amounts which the customer becomes entitled to whenever a service level is not achieved.[134] There are a number of ways in which service credits can be calculated, such as percentage rebates from the services charges for each percentage point that the service provision falls below the service level target or the use of service credit points across a range of service level measures which are then converted into service credits.[135] The purpose of this mechanism is to focus the vendor's attention on the parts of service that are most important to the customer and to drive good performance.[136]

Sole and Exclusive Remedy

The contract should specifically state whether service credits are an exclusive or non-exclusive remedy for any given performance failure.[137] From the customer's perspective, service credits are rarely sufficient as a sole and exclusive remedy because the amounts paid out are generally capped at a low sum and would not be sufficient to reimburse the customer's losses.[138] Thus, it is important to ensure that the contract states that other remedies will also be available where a service level is breached.[139] If the drafting is silent, service credits drafted as liquidated damages are likely to be interpreted as an exclusive remedy.[140]

Negotiated outcomes of these issues in the agreement typically fall somewhere between the following extremes:

- To treat the credit as a price adjustment reflecting the reduced value of the services received, with the customer also entitled to seek damages for breach;
- To treat the service credits as liquidated damages and the sole financial responsibility available to the customer;
- The service credit is treated as a price adjustment, but if damages are also sought, the service credit will be deducted from the damages;
- The customer has a period to choose whether it will either seek damages or accept the service credit;
- The service credit is treated as the sole financial remedy provided that the performance is no worse than a specified minimum threshold, but if performance goes below the minimum threshold, then damages may also be sought; and

[133] Fiona Maclean and Elizabeth Purcell, Latham & Watkins LLP, *Service Levels and Service Credit Schemes in Outsourcing*, Westlaw, USA (National/Federal)
[134] https://www.scl.org/articles/2067-back-to-basics-service-levels-and-service-credits
[135] *Id.*
[136] Maclean, *supra* note 133.
[137] *Id.*
[138] *Id.*
[139] *Id.*
[140] *Id.*

- The service credit is treated as the sole financial remedy but if the customer terminates for breach, then damages may also be sought.[141]

Service Credit Caps

Service credits are frequently "capped" at an overall percentage of the monthly or annual service charges.[142] If the contract is structured so that the costumer has a common-law right to recover actual losses in the event that the level of performance falls below the service level/service credit threshold, then the customer's position in these circumstances can be more favorable than if there is an uncapped service credit mechanism.[143] Any such uncapped service credit mechanism is likely to operate as a limit on the amount that the customer can recover in the event of a breach.[144] There are evolving market standards for the level of the cap (typically 5% to 20% of fees payable in the relevant period) but the actual level likely to be agreed on depends on many factors including:

- The aggressiveness of the performance standards;
- Whether any failure automatically leads to a credit;
- Whether the vendor has the possibility of earning back service credits for good service in other measurement periods; and
- The vendor's comfort of risk.[145]

In extreme cases, a customer may believe that is has obtained an above market standard and exceptionally strong contract position, while in reality it may be paying a premium in the charges which counterbalance any applicable service credits. This could actually reduce the vendor's incentive to perform while increasing the cost of deal.[146]

Multipliers and Weightings

In order to incentivize the rectification of the root causes of problems, service credit regimes frequently include mechanisms which impose multipliers on the service credits that are payable in the event that problems re-occur within particular timescales.[147] The intention is to prevent the vendor from behaving as though small lapses in service are a part of its overheads.[148]

Further, given that the purpose of service credits is to focus the vendor's attention on the aspects of the service that are most important to the customer, service credit mechanisms often contain a weighting mechanism apportioning larger sized credits to

---

[141] *Id.*
[142] https://www.scl.org/articles/2067-back-to-basics-service-levels-and-service-credits
[143] *Id.*
[144] *Id.*
[145] Maclean, *supra* note 133.
[146] *Id.*
[147] https://www.scl.org/articles/2067-back-to-basics-service-levels-and-service-credits
[148] *Id.*

some service levels rather than others.[149] The customer's priorities are likely to change over the term (whether because of a change in business focus or in order to respond to poor performance by the vendor in particular areas) so the more sophisticated mechanisms include a method by which the customer can elect to reallocate the weightings between service levels on giving reasonable notice.[150]

Termination

Termination of a contract is allowed when one party breaches the service level requirements.[151] However, this must be a material breach, going to the root of the contract.[152] Therefore, a temporary dip in the service level which causes minimal damages is not usually considered to be material breach.[153] However, when a vendor is providing a continued service, which may vary greatly in quality, it becomes difficult to determine the exact point at which the parties have a right to terminate.[154]

On a technology vendor agreement, it is usually in the customer's interest to specify what constitutes a material breach.[155] At the time of contracting, the parties should identify and define the basic functionality the service is intended to achieve.[156] By contract, the customer may specify what "core" functionality must be achieved by the vendor; and if the vendor fails to implement that core functionality, that failure is a material breach.[157]

In order to ensure that the court will support the customer's termination when a material breach occurs, it is best to do the following:

- Clearly identify the specific events that constitute a material breach;
- The agreement should set forth a notice requirement prior to terminating the contract for a material breach event;
- In addition to the specific material breach provision, the contract should also contain general breach of contract terms. The agreement should include operational standards that must be met in measuring performance;
- When defining the standards of performance, avoid using ambiguous terms. Common examples of terms to avoid include "industry standard," "appropriate," or "best practice;"
- Set forth service levels that allow you the ability to terminate the contract if performance falls below a defined standard.[158]

---

[149] Maclean, *supra* note 133.
[150] *Id.*
[151] https://racolblegal.com/calculating-liability-in-service-level-agreements/#_ftn10
[152] *Id.*
[153] *Id.*
[154] *Id.*
[155] https://www.pillsburylaw.com/images/content/1/0/v2/1000/BusinessLawNews-Green-2014Issue4.pdf
[156] *Id.*
[157] *Id.*
[158] http://marell-lawfirm.com/defining-material-breach-contract/

Although there are few cases that involve termination of service level agreements, one such case that has come to the forefront of how courts will interpret master service agreements is *State v. Int'l Bus. Machines Corp., 51 N.E.3d 150 (Ind. 2016)*. In December 2006, the State of Indiana ("State") and International Business Machines Corporation ("IBM") entered into a $1.3 billion Master Services Agreement ("MSA") to "modernize and improve" the State's welfare system.[159] The goal of the MSA was to establish service and call centers for processing welfare applications, enable remote electronic access to the welfare system, provide the State with an electronic document system, establish systems to prevent fraud and to improve Indiana's welfare-to work record.[160] The State terminated the MSA less than three years into the agreement, citing IBM's performance issues.[161] Both parties sued the other for breach of contract.[162]

Looking at the MSA as a whole and in light of the benefits received by the State, the trial court found that the State failed to prove that the breach was material.[163] The Court of Appeals reversed the trial court's decision on the issue of material breach, concluding that IBM's breach went to the "heart of the contract" which the Court of Appeals determined was defined by the policy objectives of the MSA.[164] The trial court and the Court of Appeals used the Restatement (Second) of Contract §241 factors for analyzing the material breach.[165] The Supreme Court of Indiana ("Supreme Court") held that "when a contract sets forth a standard for assessing the materiality of a breach, that standard governs" and that only when such a provision is absent "does the common law, including the Restatement, apply."[166] The Supreme Indiana held that IBM materially breached the MSA and reversed the trials court's finding that there was no material breach.[167]

The Supreme Court held that the trial court erred when it concluded that the State's dissatisfaction with IBM's performance did not support a claim of breach.[168] Specifically, the Supreme Court of Indiana looked to an MSA provision that stated, "A breach is material if it is 'material considering this Agreement as a whole.'"[169] The MSA further provided that "a series of breaches, none of which individually constitute[d] a breach of the Agreement may nevertheless 'collectively constitute a breach of this Agreement which is material when considering this Agreement as a whole…'"[170] Thus, the Supreme Court

---

[159] *State v. Int'l Bus. Machines Corp.*, 51 N.E.3d 150, 153 (Ind. 2016).
[160] *Id.*
[161] *Id.* at 152.
[162] *Id.*
[163] *Id.*
[164] *Id.*
[165] *Id.*
[166] *Id*. at 153.
[167] *Id.* at 158.
[168] *Id.* at 163.
[169] *Id.*
[170] *Id*.

reasoned that although the State's dissatisfaction might not alone be enough to constitute a material breach, it could constitute a material breach along with other breaches.

The Supreme Court further held that the trial court erred when it found that "IBM's failure to meet timeliness metrics did not constitute a material because 'liquidated damages were paid in lieu of performance and provided IBM with an alternative means of performance that was satisfied by payment (which payment is undisputed).'"[171] The Supreme Court reasoned that the plain language of the MSA provided that the State may pursue its termination rights, including its right to for-cause termination for a material breach or "a series of breaches that collectively constitute a material breach."[172] Therefore, the payment of liquated damages did not excuse IBM's breach and thus the trial court should have considered IBM's "consistent failure to meet certain timeliness metrics in determining whether IBM materially breached the MSA."[173]

The Supreme Court also held that the economic downturn, natural disasters, and surge in Healthy Indiana Plan (HIP) applications should not have impacted the trial court's analysis of IBM's material breach.[174] One of the Material Assumptions in the MSA was that there would not be an economic downturn in Indiana.[175] IBM could request changes to the Material Assumptions "solely pursuant to the Change Order Process."[176] IBM did not request a Change and thus the Supreme Court of Indiana held that IBM could not use the economic downturn as an excuse for nonperformance.[177] Further, IBM did not provide notice of a natural disaster in Indiana and accordingly the Supreme Court held that IBM could not use flooding as an excuse for non-performance.[178] Finally, the Supreme Court held that the trial court should not have considered the HIP applications when determining whether IBM materially breached the MSA because IBM was compensated for the Change to the increase in applications.[179] Thus, the HIP applications should not be used as a double remedy for more fees for increased scope of work and as an excuse for performance issues.[180]

IBM also argued that the State terminated the MSA for reasons other than IBM's material breach because on the day the termination was announced to the public, the Governor of Indiana praised IBM for their work.[181] The Supreme Court concluded that it does matter what State officials say about terminating the contract because only the written terms of the contract matter.[182] Thus, the Supreme Court held that the trial court

---

[171] *Id.* at 164.
[172] *Id*.
[173] *Id.*
[174] *Id.*
[175] *Id.*
[176] *Id.*
[177] *Id.*
[178] *Id.*
[179] *Id.* at 165.
[180] *Id.*
[181] *Id.* at 166.
[182] *Id.*

should not have considered whether the State had other reasons for terminating the MSA.[183]

Finally, the Supreme Court rejected the trial court's analysis that the benefits provided to the State by IBM ameliorated the material breach.[184] The Supreme Court determined that balancing the benefits received by the State with IBM's performance failings was "not the appropriate standard for determining whether there [was] a material breach" because the standard laid out in the MSA is to look to "a series of breaches, none of which individually constitute a breach of the Agreement [which] may nevertheless 'collectively constitute a breach of [the] Agreement which is material when consider [the] Agreement as a whole…'"[185] Thus, the trial court erred in finding that the "benefits received by the State precluded a finding that IBM materially breached the MSA."[186]

[183] *Id.*
[184] *Id*.
[185] *Id.*
[186] *Id.* at 168.

APPENDIX A
SAMPLE PROVISIONS

Specific Provisions

Cost Sharing

Lead Generation or Call Center

We reserve the right to provide, and/or contract with a third-party to develop and operate, a call center or other sales inquiry/sales generating service, and/or to provide or contract with third parties, including Internet-based marketing companies, to provide, lead generation services to our network of [NAME OF FRANCHISE SYSTEM] Businesses. Charges and fees for a call center and/or lead generation services may include one-time set-up fees per business, monthly fees, and/or per-call or per-lead fees. We expect that the fees charged will be to reimburse us for costs associated with these services, and/or to pay third parties for these services. We may require you to use the call center or lead generation services, or we may only recommend that you do. If you participate and use the call center or lead generation services, you must comply with all rules, policies, and requirements specified by the provider and us regarding such services. We reserve the right to add to, modify, or eliminate approved, recommended, or required products, services, or suppliers at any time.

Approved Supplier

The Franchisee agrees that it will purchase only those products, goods, machinery, signs, software, supplies, equipment and services (sometimes referred to in this Agreement as "goods and services") which are to be used or sold by the Franchisee that are approved in writing by Franchisor and which Franchisor determines must meet the standards of quality and uniformity required to protect the valuable goodwill and uniformity symbolized by and associated with the Marks and the System. These goods and services may only be purchased from suppliers, approved in writing by Franchisor. Franchisor periodically may modify the lists of approved goods, services and suppliers, and the Franchisee will comply with such modified lists of approved goods, services and suppliers.

Approved Products, Distributors and Suppliers

We have developed or may develop standards and specifications for types, models and brands of required Operating Assets, and other products. We reserve the right from time to time to approve specifications or suppliers and distributors of the products that meet our reasonable standards and requirements. If we do so, you agree to purchase only such products meeting those specifications, and if we require it, only

from distributors and other suppliers we have approved, including ourselves or our affiliates.

We may designate a single distributor or supplier (collectively, "**supplier**") for any product, service, equipment, supply or material and may approve a supplier or distributor only as to certain products. The designated supplier may be us or an affiliate of ours.

We and our affiliates may receive payments from suppliers on account of such suppliers' dealings with you and other franchisees, and may use any amounts received without restriction and for any purpose we and our affiliates deem appropriate. We may concentrate purchases with one or more suppliers or distributors to obtain lower prices or advantageous advertising support or services. Approval of a supplier or distributor may be conditioned on requirements relating to product quality, prices, consistency, reliability, financial capability, labor relations, customer relations, frequency of delivery, concentration of purchases, standards of service, including prompt attention to complaints, or other criteria and may be temporary, pending our continued evaluation of the supplier or distributor from time to time. You or any other franchisee shall not be an approved vendor to the [NAME OF FRANCHISE SYSTEM].

Approved Suppliers

Recognizing that the Approved Services must conform to Franchisor's standards and specifications, Franchisee hereby agrees to purchase all goods and services used in the Franchised Business only from Franchisor or from other suppliers approved or designated in writing by Franchisor (which may include or be limited to Franchisor or its affiliates). If Franchisee desires to purchase a good or service used in the Franchised Business from an alternative supplier, Franchisee must comply with the alternative supplier approval requirements described in the Operations Manual.

Franchisee must purchase and use Franchisor's designated software(s) and technology platforms to operate the Franchised Business, which Franchisee must acquire from Franchisor, its affiliate, or a supplier designated by Franchisor. Franchisor has the right to specify or require that certain brands, types, makes, and/or models of communications, computer systems, and hardware to be used by, between or among franchisees, and in accordance with Franchisor's standards, including back office systems, data, audio, video (including managed video security surveillance), telephone, voice messaging, retrieval, and transmission systems for use at the Franchised Business; physical, electronic, and other security systems and measures; printers and other peripheral devices; archival back-up systems; internet access mode (e.g., form of telecommunications connection) and speed; technology used to enhance and evaluate the consumer experience; connectivity service; and supply-chain management programs. Franchisor may require Franchisee to sign a software access or license agreement in connection with Franchisee's use of such required software programs.

Franchisee must pay Franchisor or its designated supplier the then-current fees for use of any designated software or technology, including any license, maintenance, support or other fees. Franchisor reserves the right to change, update, replace or eliminate the required software or require new software from time to time at Franchisee's expense. Franchisee must use, and at Franchisor's discretion, pay for all future updates, supplements and modifications to the required software programs

Franchisee hereby acknowledges with respect to Franchisee's use of Franchisor's or a third party's software for operating the System that Franchisee is responsible for complying with all local, state and federal laws and the accuracy of all information entered into, contained in, generated by or accessible from such software. Franchisee further acknowledges that Franchisor disclaims any and all warranties relating to such software and Franchisee's use thereof, including, but not limited to, warranties of merchantability or fitness for a particular purpose. Franchisee is solely responsible for protecting itself from disruptions, Internet access failures, Internet content failures and attacks by hackers and other unauthorized intruders and Franchisee waives any and all claims Franchisee may have against Franchisor as the direct or indirect result of such disruptions, failures or attacks.

Information Technology Requirements.

If required by the Franchisor, the Franchisee shall at its sole expense acquire, license, use and maintain, as the case may be, any computer system, software or other information technology systems and services, including Internet service, meeting the Franchisor's standards and specifications. The Franchisee's use of such information technology meeting the Franchisor's standards and specifications may be required and may be necessary to permit the Franchisee to fully utilize the System, obtain certain services from the Franchisor and communicate with the Franchisor, Clients and others.

Technology Fees/Fund

The Franchisee will, for the entire term of this Agreement, remit to Franchisor weekly Technology Fees of ___% of the Franchisee's weekly Gross Revenues which are received, billed, or generated by, as a result of, in connection with or from the Franchised Business operated pursuant to this Agreement (the "Technology Fee"). The weekly Technology Fees paid by the Franchisee to Franchisor will be deposited in the Technology Fund and will not be refundable to the Franchisee under any circumstances. Franchisor reserves the right to increase the amount of the weekly Technology Fee. Any increase in the weekly Technology Fee will not take effect until the Franchisee has been given at least 90 days prior written notice of the increase. Any increase will not exceed the maximum __% of the Franchisee's weekly Gross Revenues.

Use of Technology Fund

Payments to [NAME OF FRANCHISE SYSTEM] Technology Fund by the Franchisee and any other [NAME OF FRANCHISE SYSTEM] franchises will be used by Franchisor to purchase and pay for the research, development and utilization of technologies, in order to give [NAME OF FRANCHISE SYSTEM] franchises a competitive advantage in operational efficiency; information management; any and all other technology Franchisor deems beneficial for the [NAME OF FRANCHISE SYSTEM] System; and any administrative costs and expenses related to the foregoing. Funds in [NAME OF FRANCHISE SYSTEM] National Technology Fund will be used to pay for all long distance telephone charges, office rental, furniture, fixtures and equipment, leasehold improvements, personnel, salaries, travel costs, office supplies, collection costs (including without limitation attorneys' fees) incurred in attempting to collect past-due weekly Technology Fees from franchisees, and all other administrative costs associated with an incurred in connection with [NAME OF FRANCHISE SYSTEM] Technology Fund. [NAME OF FRANCHISE SYSTEM] National Technology Fund will be administered and controlled exclusively by Franchisor. Franchisor will have the absolute and unilateral right to determine when, how, and where any Funds in [NAME OF FRANCHISE SYSTEM] Technology Fund will be spent. Franchisor will have no fiduciary duty to the Franchisee with respect to collection or expenditure of the weekly Technology Fees, and any technology fund will not be a trust or escrow account. Any [NAME OF FRANCHISE SYSTEM] Businesses operated by Franchisor will be required to contribute to [NAME OF FRANCHISE SYSTEM] Technology Fund in the same manner as franchisees.

Technology Fee

Franchisor reserves the right to charge and, if implemented, Franchisee agrees to pay Franchisor the then-current "Technology Fee." The Technology Fee defrays the indirect costs of creating, implementing and supporting new and existing software and technology platforms such as hosting, integration development, server infrastructure and support that are often not included in direct costs of those software and technology platforms. After Franchisor implements the Technology Fee, the Technology Fee may be adjusted at any time with sixty (60) days' prior written notice to Franchisee; provided that Franchisor will not increase the Technology Fee by more than twenty-five percent (25%) each calendar year

Franchisee Advisory Council

In order to provide a forum to exchange ideas and information between the Franchisor and [NAME OF FRANCHISE SYSTEM] Franchisees, the Franchisor reserves the right to establish an advisory council (the "Advisory Council"), the term of reference of which shall be contained in the Manual and which shall be implemented in good faith and in accordance with reasonable commercial standards. The terms of reference shall

set out the terms and conditions upon which the Franchisee may be eligible to participate on the Advisory Council.

Changes to the System

The Franchisee recognizes that variations and additions to the System will be required from time to time to preserve and enhance the public image of the System, to accommodate changing consumer trends and to ensure the continuing efficiency of the System generally. The Franchisee acknowledges and agrees that the franchisor may, from time to time, upon written notice to the Franchisee add to, subtract from or otherwise change the System, through the Manual or otherwise in writing. The changes to the System may include, without limitation, the adoption of new or modified trademarks and trade names, new products, services, renovations, equipment, fixtures, furnishings, and technology solutions. The Franchisee agrees to promptly accept, implement, use and display all such changes to the System in the conduct of the Franchised Business, at the Franchisee's sole cost.

Changes to the Operations Manual

The Franchisor shall have the right to add to, modify, withdraw from or otherwise revise the provisions of the Manual from time to time as provided for in this Agreement or to maintain the goodwill associated with the System and the Trademarks, provided that (i) no such revision shall alter unreasonably the Franchisee's fundamental rights under this Agreement and (ii) each revision shall be made in good faith and in accordance with reasonable commercial standards.

APPENDIX B

	VENDOR VETTING QUESTIONNAIRE
1	Is the company willing to sign and comply with the terms of a Business Associate Agreement (BAA) under HIPPA, GDPR Data Processing Agreement, or other standard contractual provisions in order to comply with applicable law
2	How does your solution enable compliance with applicable Canadian privacy laws (e.g. PIPEDA)?
3	How does your solution enable compliance with applicable privacy laws in the United States (e.g. CCPA, HIPAA, CAN-SPAM, etc.)?
4	How does your solution enable compliance with applicable international privacy laws (e.g. GDPR, APEC)?
5	Summarize and provide copies of the company's information security policies and procedures, specifically including: 1) practices related to encryption of internal and external transmissions; and ensuring integrity in the storage of data
6	Summarize and provide copies of the company's privacy policies and procedures, specifically including practices related to third-party data sharing
7	Summarize and provide copies of the company's data security incident and breach handling policies and procedures, specifically including practices to identify, mitigate, and provide notifications
8	Summarize and provide information regarding whether the company maintains any EU/Swiss safe harbors, Privacy Shield certification, or other certification related to its privacy or security practices
9	Summarize the company's customer data hosting locations that would be utilized
10	Does your company have a designated compliance, privacy, security officer? Please provide the name and title of such individual.
Legal Contractual Considerations	

11	It is company's position that the right to use of its customer data entered into the system, or collected by the system on its behalf, must be authorized by company and the right to such use will cease upon termination of any agreement. If you are not able to agree to such terms, please indicate the exceptions.
12	Please list all current or past litigation or administrative investigations, actions, rulings, notifications, or orders in the last 5 years relating in any way to your product, services, or your compliance with laws/regulations or contracts for such products and services.
13	Provide a listing of applicable insurance coverage, including Commercial General Liability and Cyber Insurance maintained with relevant coverage limits.
14	What assurances or guarantees is the company willing to provide regarding the availability of data and restoration of data in the event that data integrity or availability is compromised.
15	Describe your software licensing process, and any license options. Include a copy of your typical license agreement.
17	Do you understand that the license or provision of services may include _____ franchise network of independently owned and operated businesses and that this may, consequently, require the sublicensing of services or expansion of a standard definition of “Users”?

APPENDIX C

DATA SECURITY ADDENDUM

This Data Protection Addendum ("Addendum") forms part of the INSERT AGREEMENT NAME ("Principal Agreement") between: INSERT COMPANY NAME a INSERT COMPANY STATE corporation with offices located at INSERT COMPANY ADDRESS (“Company”) and INSERT VENDOR NAME an INSERT VENDOR STATE corporation with offices located at INSERT VENDOR ADDRESS ("Service Provider").

The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement. Except as modified below, the terms of the Principal Agreement shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Principal Agreement. Except where the context requires otherwise, references in this Addendum to the Principal Agreement are to the Principal Agreement as amended by, and including, this Addendum.

1. Definitions.

"**Authorized Employees**" means Service Provider's employees who have a need to know or otherwise access Personal Information to enable Service Provider to perform its obligations under the Principal Agreement.

"**Authorized Persons**" means (i) Authorized Employees; and (ii) Service Provider's contractors, agents, own service providers, and auditors who have a need to know or otherwise access Personal Information to enable Service Provider to perform its obligations under the Principal Agreement, and who are bound in writing by confidentiality and other obligations sufficient to protect Personal Information in accordance with the terms and conditions of this Addendum.

"**Personal Information**" means information provided to Service Provider by or at the direction of Company, Company’s affiliates and/or Company’s franchised or master franchised businesses. Information which is created or obtained by Service Provider on behalf of Company, Company’s affiliates and/or Company’s franchised or master franchised businesses or information to which access was provided to Service Provider by or at the direction of Company, Company’s affiliates and/or Company’s franchised or master franchised businesses in the course of Service Provider's performance under this Addendum that: (i) identifies or can be used to identify an individual (including, without

limitation, names, signatures, addresses, telephone numbers, email addresses, and other unique identifiers); or (ii) can be used to authenticate an individual (including, without limitation, employee identification numbers, government-issued identification numbers, passwords or PINs, user identification and account access credentials or passwords, financial account numbers, credit report information, student information, biometric, health, genetic, medical, or medical insurance data, and other personal identifiers). Company's business contact information is not by itself deemed to be Personal Information.

"**Security Breach**" means (i) any act or omission that compromises either the security, confidentiality, or integrity of Personal Information or the physical, technical, administrative, or organizational safeguards put in place by Service Provider, or by Company should Service Provider have access to Company's systems, that relate to the protection of the security, confidentiality, or integrity of Personal Information, or a breach or alleged breach of this Addendum relating to such privacy and data security practices. Without limiting the foregoing, a compromise shall include any unauthorized access to or disclosure or acquisition of Personal Information.

"**Unauthorized Third Party**" means (i) any person or party that has access to Personal Information, provided by Company, to Service Provider that is not an Authorized Employee or Authorized Person. government entities are excluded from this definition when they are granted access to Personal Information, as required by applicable law.

2. Standard of Care.

(a) Service Provider acknowledges and agrees that, in the course of its engagement by Company, Service Provider may create, receive, or have access to Personal Information. Service Provider shall comply with the terms and conditions set forth in this Addendum in its creation, collection, receipt, transmission, storage, disposal, use, and disclosure of such Personal Information and be responsible for any unauthorized creation, collection, receipt, transmission, access, storage, disposal, use, or disclosure of Personal Information under its control or in its possession by all Authorized Employees and Authorized Persons. Service Provider shall be responsible for, and remain liable to, Company for the actions and omissions of all Authorized Persons that are not Authorized Employees concerning the treatment of Personal Information as if they were Service Provider's own actions and omissions.

(b) In recognition of the foregoing, Service Provider agrees and covenants that it shall:

(i) keep and maintain all Personal Information in strict confidence, using such degree of care as is appropriate to avoid unauthorized access, use, or disclosure;

(ii) Ensure that Authorized Employees and Authorized Persons have received appropriate training on their responsibilities regarding access to Company's Personal Information.

(iii) Perform due diligence on Authorized Employees and Authorized Persons, such as background checks, before granting access to Personal Information.

(iv) not create, collect, receive, access, or use Personal Information in violation of law;

(v) use and disclose Personal Information solely and exclusively for the purposes for which the Personal Information, or access to it, is provided pursuant to the terms and conditions of this Addendum, and not use, sell, rent, transfer, distribute, or otherwise disclose or make available Personal Information for Service Provider's own purposes or for the benefit of anyone other than Company, in each case, without Company's prior written consent; and

(vi) not, directly or indirectly, disclose Personal Information to any person other than its Authorized Employees or Authorized Persons without Company's prior written consent unless and to the extent required by government authorities or as otherwise, to the extent expressly required, by applicable law, in which case, Service Provider shall (A) notify Company before such disclosure and provide Company reasonable assistance as may be required for Company to seek a protective order; (B) be responsible for and remain liable to Company for the actions and omissions of such Unauthorized Third Party concerning the treatment of such Personal Information as if they were Service Provider's own actions and omissions; and (C) require the Unauthorized Third Party that has access to Personal Information to execute a written agreement agreeing to comply with the terms and conditions of this.

3. Information Security.

(a) Service Provider represents and warrants that its creation, collection, receipt, access, use, storage, disposal, and disclosure of Personal Information does and will comply with all applicable federal, state, and foreign privacy and data protection laws, as well as all other applicable regulations and directives.

(b) Service Provider shall implement and maintain a written information security program including appropriate policies, procedures, and risk assessments that are reviewed at least annually.

(c) Without limiting Service Provider's obligations under Section 3(a), Service Provider shall implement administrative, physical, and technical safeguards to protect Personal Information from unauthorized access, acquisition, or disclosure, destruction, alteration, accidental loss, misuse, or damage that are no less rigorous than accepted industry practices including the International Organization for Standardization's standards: ISO/IEC 27001, or other applicable industry standards for information security, and shall ensure that all such safeguards, including the manner in which Personal Information is created, collected, accessed, received, used, stored, processed, disposed of, and disclosed, comply with applicable data protection and privacy laws, as well as the terms and conditions of this Addendum.

If, in the course of its engagement by Company, Service Provider has access to or will collect, access, use, store, process, dispose of, or disclose credit, debit, or other payment cardholder information, Service Provider shall at all times remain in compliance with the Payment Card Industry Data Security Standard ("PCI DSS") requirements, including remaining aware at all times of changes to the PCI DSS and promptly implementing all procedures and practices as may be necessary to remain in compliance with the PCI DSS, in each case, at Service Provider's sole cost and expense.

(d) At a minimum, Service Provider's safeguards for the protection of Personal Information shall include: (i) limiting access of Personal Information to Authorized Employees and Authorized Persons; (ii) securing business facilities, data centers, paper files, servers, backup systems, and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability; (iii) implementing network, application, database, and platform security; (iv) securing information transmission, storage, and disposal; (v) implementing authentication and access controls within media, applications, operating systems, and equipment; (vi) encrypting Personal Information stored on any mobile media; (vii) encrypting Personal Information transmitted over public or wireless networks; (viii) strictly segregating Personal Information from information of Service Provider or its other Company information so that Personal Information is not commingled with any other types of information; (ix) conducting risk assessments, penetration testing, and vulnerability scans and promptly implementing, at Service Provider’s sole cost and expense, a corrective action plan to correct any issues that are reported as a result of the testing; (x) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; and (xi) providing appropriate privacy and information security training to Service Provider's employees.

(e) During the term of each Authorized Employee's employment by Service Provider, Service Provider shall at all times cause such Authorized Employees to abide strictly by Service Provider's obligations under this Addendum. Service Provider further agrees that it shall maintain a disciplinary process to address any unauthorized access, use, or disclosure of Personal Information by

any of Service Provider's officers, partners, principals, employees, agents, or contractors. Upon Company's written request, Service Provider shall promptly identify for Company in writing all Authorized Employees as of the date of such request.

4. Security Breach Procedures.

(a) Service Provider shall:

(i) provide Company with the name and contact information for an employee of Service Provider who shall serve as Company's primary security contact and shall be available to assist Company twenty-four (24) hours per day, seven (7) days per week as a contact in resolving obligations associated with a Security Breach;

(ii) notify Company of a Security Breach as soon as practicable, but no later than twenty-four (24) hours after Service Provider becomes aware of it; and

(iii) notify Company of any Security Breaches by emailing Company at EMAIL ADDRESSES, with a copy by email to Service Provider's primary business contact within Company.

(b) Immediately following Service Provider's notification to Company of a Security Breach, the parties shall coordinate with each other to investigate the Security Breach. Service Provider agrees to fully cooperate with Company in Company's handling of the matter, including, without limitation: (i) assisting with any investigation; (ii) providing Company with physical access to the facilities and operations affected; (iii) facilitating interviews with Service Provider's employees and others involved in the matter; and (iv) making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law, regulation, industry standards, or as otherwise reasonably required by Company.

(c) Service Provider shall at its own expense use best efforts to immediately contain and remedy any Security Breach and prevent any further Security Breach, including, but not limited to taking any and all action necessary to comply with applicable privacy rights, laws, regulations, and standards. Service Provider shall reimburse Company for all actual costs incurred by Company in responding to, and mitigating damages caused by, any Security Breach, including all costs of notice and/or remediation pursuant to Section 4(d).

(d) Service Provider agrees that it shall not inform any third party, with the exception of outside counsel or an insurance provider, of any Security Breach without first obtaining Company's prior written consent, other than to inform a complainant that the matter has been forwarded to Company's legal counsel. Further, Service Provider agrees that Company shall have the sole right to determine: (i) whether notice of the Security Breach is to be provided to any

individuals, regulators, law enforcement agencies, consumer reporting agencies, or others as required by law or regulation, or otherwise in Company's discretion; and (ii) the contents of such notice, whether any type of remediation may be offered to affected persons, and the nature and extent of any such remediation.

(e) Service Provider agrees to maintain and preserve all documents, records, and other data related to any Security Breach.

(f) Service Provider agrees to reasonably cooperate at its own expense with Company in any litigation, investigation, or other action deemed reasonably necessary by Company to protect its rights relating to the use, disclosure, protection, and maintenance of Personal Information.

(g) In the event of any Security Breach, Service Provider shall promptly use its best efforts to prevent a recurrence of any such Security Breach.

5. Oversight of Security Compliance. Upon Company's written request, to confirm Service Provider's compliance with this Addendum, as well as any applicable laws, regulations, and industry standards, Service Provider grants Company or, upon Company's election, a third party on Company's behalf, permission to perform an assessment, audit, examination, or review of all controls in Service Provider's physical and/or technical environment in relation to all Personal Information being handled and/or services being provided to Company pursuant to the Principal Agreement. Service Provider shall fully cooperate with such assessment by providing access to knowledgeable personnel, physical premises, documentation, infrastructure, and application software that processes, stores, or transports Personal Information for Company pursuant to the Principal Agreement. In addition, upon Company's written request, Service Provider shall provide Company with the results of any audit by or on behalf of Service Provider performed that assesses the effectiveness of Service Provider's information security program as relevant to the security and confidentiality of Personal Information shared during the course of the Principal Agreement.

6. Return or Destruction of Personal Information. At any time during the term of the Principal Agreement, at Company's written request, Service Provider shall, and shall instruct all Authorized Employees and Authorized Persons to, promptly return to Company all copies, whether in written, electronic, or other form or media, of Personal Information in its possession or the possession of such Authorized Employees. Service Provider shall comply with all directions provided by Company with respect to the return or disposal of Personal Information.

7. Equitable Relief. Service Provider acknowledges that any breach of its covenants or obligations set forth in this Addendum may cause Company irreparable harm for which monetary damages would not be adequate compensation and agrees that, in the event of such breach or threatened breach, Company is entitled to seek equitable relief, including a restraining order, injunctive relief, specific performance, and any other relief that may be available from any court, in addition to any other remedy to which Company may be entitled at law or in equity. Such remedies shall not be deemed

to be exclusive but shall be in addition to all other remedies available at law or in equity, subject to any express exclusions or limitations in this Addendum to the contrary.

8. Indemnification. Service Provider shall defend, indemnify, and hold harmless Company and our subsidiaries, affiliates, and our respective officers, directors, employees, agents, successors, and permitted assigns (each, a "**Company Indemnitee**") from and against all losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, penalties, fines, costs, or expenses of whatever kind, including reasonable attorneys' fees, the cost of enforcing any right to indemnification hereunder, and the cost of pursuing any insurance providers, arising out of or resulting from any third-party claim against any Company Indemnitee arising out of or resulting from Service Provider's failure to comply with any of its obligations under this Addendum.

9. Termination of Agreement

(a) Company may terminate the Principal Agreement, by written notice, if it determines, in its sole discretion, that Service Provider has breached any provision of this Addendum. Any such termination will be effective immediately or at such other date specified in Company's notice of termination.

(b) Obligations on Termination

(i) Service Provider will, return to Company or destroy all of Company's Personal Information in whatever form or medium, including all copies thereof and all data, compilations, and other works derived there from that allow identification of any individual who is a subject of Company's Personal Information. Service Provider will require Authorized Persons and Authorized Employees, to which Service Provider has disclosed Company's Personal Information as permitted by Section 2(a) of this Addendum, to return to Service Provider (so that Service Provider may return it to Company) or destroy all of Company's Personal Information in whatever form or medium received from Service Provider, including all copies thereof and all data, compilations, and other works derived therefrom that allow identification of any individual who is a subject of Company's Personal Information, and certify on oath to Service Provider that all such information has been returned or destroyed. Service Provider will complete these obligations as promptly as possible, but not later than 60 days following the effective date of the termination or other conclusion of the Principal Agreement.

(ii) Service Provider's obligation to protect the privacy and safeguard the security of Company's Personal Information as specified in this Addendum will be continuous and survive termination or other conclusion of the Principal Agreement and this Addendum.

(iii) Service Provider's other obligations and rights, and Company's obligations and rights upon termination or other conclusion of

the Principal Agreement will be those set out in the Principal Agreement or this Addendum as obligations or rights surviving the termination of the Principal Agreement.