MOBILE APPS, REMOTE ORDERING, AND LOYALTY PROGRAMS; RISKS AND OPPORTUNITIES

Gary R. Batenhorst
Cline Williams Wright Johnson & Oldfather, L.L.P.
Omaha, NE

Lindsey Cooper
Franchise World Headquarters, LLC
Milford, CT

Daniel Graham
Perkins Coie LLP
Denver, CO

October 16-18, 2019
Denver, CO

©2019 American Bar Association
# Table of Contents

I. INTRODUCTION ............................................................................................................. 1

II. SOFTWARE DEVELOPMENT AND LICENSE AGREEMENTS .............................................. 2
   A. Developer Selection ........................................................................................... 2
   B. Scope of Mobile App Programs .......................................................................... 2
   C. Developing a Timeline to Roll Out a Mobile App ................................................ 4
   D. Negotiating Development and License Agreements .......................................... 5
       1. Testing .................................................................................................... 5
       2. Intellectual Property ................................................................................ 5
       3. Confidential Information and Trade Secrets ........................................... 6
       4. Payment Terms ...................................................................................... 6
       5. Legal Compliance ................................................................................... 7
       6. Representations and Warranties ............................................................ 7
       7. Indemnification ........................................................................................ 7
       8. Defaults ................................................................................................... 8
       9. Service Level Agreements ...................................................................... 8
      10. Exclusivity ............................................................................................... 8
      11. Termination and Expiration ..................................................................... 8
   E. Integration of Apps with POS Systems ............................................................... 9
   F. Terms and Conditions of Use ............................................................................. 9
   G. Integration of Mobile Apps with Social Media Sites ............................................ 10

III. DATA PRIVACY CONCERNS ....................................................................................... 10
   A. Application of Data Privacy Statutes and Regulations .................................... 10
       1. The GDPR .............................................................................................. 11
       2. The CCPA ............................................................................................... 12
   B. Issues Related to Mobile Pay Functions in App ............................................... 13
C. Issues Concerning Data Privacy Breaches .......................................................... 14
D. The Relationship Between Terms and Conditions for Use and Data Privacy Issues .................................................................................................................... 14
E. Ownership of the Data Collected in Apps .............................................................. 15

IV. INSURANCE ISSUES ..................................................................................................... 15
V. ROLLOUT AND COMMUNICATION OF BENEFITS TO FRANCHISEES ............. 16
   A. Determine Required Technology Updates for Franchisee Participation in Mobile App Program .............................................................................................................. 17
   B. Scope the Cost for Franchisees to Implement Mobile App Program .................... 17
   C. Determine If Program is Voluntary Or Mandatory .............................................. 18
   D. Franchise Disclosure Implications .................................................................... 18
   E. Timeline For Franchisee Rollout ........................................................................ 19
   F. Training for Franchisees ..................................................................................... 20

VI. FRANCHISEE COMPLIANCE WITH MOBILE APP PROGRAM REQUIREMENTS .... 20
   A. Defining Participation Requirements .................................................................. 20
   B. Sources of Mobile App Program Requirements .................................................. 21
   C. Agreements between Franchisees and the App Developer ..................................... 21
   D. Impact on Franchise Agreement and Other Documents ........................................ 22
   E. Prohibitions on Use of Unapproved Technology ................................................ 22

VII. ADA COMPLIANCE ISSUES .................................................................................. 22
    A. Application of the ADA to Mobile Apps ............................................................. 23
    B. Requirements for ADA Compliance ................................................................... 25
    C. Allocating ADA Compliance Responsibilities Between Developer and Franchisor ........................................................................................................... 26
    D. Vicarious Liability Issues .................................................................................... 27

VIII. OTHER ISSUES .................................................................................................... 27
    A. Compliance with Menu Labeling Requirements by Food Service Providers ..... 27
    B. Providing Technology to Permit Customers To Identify Food Allergy Issues ..... 29
C. Issues for Sites Marketing to Children .................................................................31
D. Application of TCPA, CSPAM, and Related Statutes ..............................................33
IX. CONCLUSION ...........................................................................................................37

BIOGRAPHIES
I. INTRODUCTION

A mobile app is a computer program or software application used on small wireless devices, such as phones, tablets, or watches. Mobile apps are everywhere. An increasingly important part of our digital lives, we have mobile apps for our banks, our supermarkets, our pharmacies, and our favorite restaurants. We use mobile apps to get our news, listen to podcasts, buy our music, and acquire other apps. Mobile apps also are important components of online ordering and customer loyalty programs. There are even mobile app franchises, such as Eazi-Apps in Great Britain and Mobile App City.

Mobile apps, online ordering, and loyalty programs provide many great opportunities for franchise systems to better promote their brands in a uniform way. One recent article suggests there are no fewer than fourteen different ways mobile apps benefit restaurant systems. Those benefits include using available technology to provide push notifications (information delivered from a software program to a device, such as a phone or tablet, without a specific request from the user) to customers located near a restaurant, better utilized customer loyalty and referral programs, labor savings at restaurants, better and faster customer service, ease in making reservations, and easier sharing of experiences (good or bad) on restaurant rating and social media sites. Robust online ordering programs and mobile apps also help franchise systems, restaurant-related or otherwise, seeking more business from millennials. Research has shown that thirty-five percent of millennials prefer ordering from restaurants from their phone or tablet, and forty percent prefer to use mobile pay options.

But with all of these opportunities come risks as well. The use of mobile apps, online ordering through a company’s website, and customer loyalty programs give franchise businesses access to a wide range of data on their customers, which subjects the franchise business to the increasing number of data privacy and cybersecurity laws. Mobile pay systems are important parts of mobile app and online order programs, but require compliance with various laws and regulations related to credit cards and financial information provided by customers.

This raises issues regarding who (franchisor or franchisee) bears the expense if violations of these laws occur, as well as issues regarding insurance coverage for potential violations such as data breaches. Compliance by online ordering websites and mobile apps with the Americans With Disabilities Act (ADA) has been the subject of an increasing number of lawsuits in recent years, a trend that shows no sign of slowing down. Restaurant franchises face issues in complying with menu labeling laws and with finding ways to enable customers to make the restaurant aware of food allergy and related issues affecting customers. Truth in advertising and other laws can also be implicated.

Franchise agreements and franchise disclosure documents often need to be revised when franchisors seek to roll out online ordering, mobile app, and loyalty programs.

---

2 Id.
3 Id.
This paper will take a closer look at the opportunities presented by online ordering, mobile apps, and loyalty programs. It also addresses the risks that must be managed in rolling out these programs.

II. SOFTWARE DEVELOPMENT AND LICENSE AGREEMENTS

A. Developer Selection

One of the most important decisions a franchisor must make in rolling out a mobile app program is the selection of the mobile app and online ordering (if applicable) software developer. Selecting an app developer can have significant implications—positive or negative—for a franchise system, so the importance of finding the right vendor cannot be overstated. In the increasingly competitive environment many franchisors face, introducing a robust app into the system can increase sales and profits for franchised and corporate locations, enhance customers' experience, and improve franchisee satisfaction with the system. On the other hand, rolling out a poor mobile app can have a strong negative impact on a franchised system. It also is important that a franchisor negotiate good agreements with an app developer that protect the franchise system while at the same time providing the developer with sufficient incentives to provide outstanding service to the franchise system. Negotiating these agreements can be a difficult and time-consuming process.

While franchisors must consider a number of factors, experience in the franchisor’s industry and experience with other franchised concepts are important to the successful development and rollout of a mobile app. For example, restaurant franchisors present big challenges for developers, who must deal with factors such as regional menu differences and menu labeling laws. In performing their due diligence on potential vendors, franchisors must look for developers with a proven record of successful rollouts that meet critical deadlines. Particularly in some industries there may be mobile app ratings services franchisors can use to determine the level of client and consumer acceptance of a developer’s apps.

Franchisors also will want to determine the stability and depth of the developer’s management and development teams and seek available information on the developer’s financial strength. Franchisors may want to obtain the names of other apps and online ordering programs developed by a prospective developer in the franchisor’s industry. One risk to this approach is that the look and feel of a franchisor’s app may resemble that of a competitor with whom the developer worked. But this risk may be outweighed by cost savings resulting from the developer’s industry experience. Franchisors can download other apps developed by a prospective developer to assess their functionality and ease of use. Franchisors also will want to seriously consider a prospective developer’s performance in interviews and presentations, asking sufficiently detailed questions to determine how developers have responded to general issues in the development process. Franchisors should also consider involving franchisees with varying degrees of technological skills and outside advertising and marketing agencies in the selection process.

B. Scope of Mobile App Programs

Along with selecting the best developer for the system, franchisors must carefully consider the features to include in the mobile app. Online ordering will be an important component of the mobile app for most retail franchises. The ability to quickly and easily place an order online is
becoming an indispensable component of the marketing strategy of many franchised retailers.\(^4\) Successful online ordering will require the app to provide easy access to and interfacing with the franchisor’s website and the point-of-sale (POS) system for each location as well as integration with secure, easy to use mobile payment programs, such as Apple Pay and Android Pay.\(^5\) It also requires the app to have a good locator component so that customers can easily find the closest locations, which gives these locations the opportunity to send push notifications of special offers to entice potential customers to patronize them.

Other services that mobile apps can provide include loyalty programs, customer relationship management (CRM) programs, digital couponing, and gift card management. The addition of these components can increase the value of the mobile app in attracting and retaining customers, but each presents operational and in some cases legal issues to address. Loyalty programs must provide easy ways for points to be added to customer accounts following purchases, for customers to see their point balances and what they can get by redeeming points, and for customers to redeem points to receive goods and services from franchised and company locations. But these loyalty programs can lead to dissatisfaction among franchisees who redeem substantial numbers of points, in many cases providing free products or services to customers who accumulated points by purchases at other locations. Franchisors need systems to address these issues. This may include the maintenance of a centralized fund, to which franchisees and the franchisor contribute, to compensate locations that have substantial imbalances in loyalty point redemptions.

Gift cards provided through a mobile app present both franchise operations and legal issues. As with loyalty points, franchisees need a mechanism for compensating a franchisee that redeems a gift card purchased at another franchisee’s location while charging the selling location. Although beyond the scope of this paper, but a significant risk to franchise systems, gift card sellers must also deal with a variety of state laws governing issues such as expiration dates and state escheat laws for expired gift cards.\(^6\)

Gift card and loyalty programs both serve as cash substitutes for customers because they can be redeemed for goods and services in company and franchised locations. As a result, they are at risk of theft and internal manipulation at retail locations and in the franchisor’s and franchisee’s offices. Franchisors and franchisees need effective internal controls in place to properly account for gift cards and loyalty points and prevent their misuse.

Digital couponing services permit retail locations to use the app to provide online coupons to their customers. With the continuing decline in print media, digital couponing is an increasingly important means for franchised businesses to provide coupons to customers. As with any coupons, franchisors must have a mechanism in place to approve certain offers and to ensure digital coupons are clear on expiration dates and the locations at which they may be redeemed.

---

\(^4\) A robust online ordering system is an important component of restaurant food delivery. The investment firm Cowen Group predicts there will be a seventy-nine percent increase in food delivery from $43 billion in 2017 to $75.9 billion in 2022. Agnes The Stubbs, *Why You Need to Take Your Restaurant Food Ordering In-House*, SOFTWARE ADVICE, https://www.softwareadvice.com/resources/online-restaurant-ordering-system-options/ (last visited July 22, 2019).


\(^6\) For a discussion of issues related to state gift card laws, see Evan M. Sauda and Emily I. Bridges, *Issuer Beware: The Varied Landscape of State “Baby-CARD” Laws*, 36 Franchise L.J. 69 (Summer 2016).
CRM programs enable locations in a franchised system to implement interactions with social media sites and to manage email communications to customers of franchised and company locations. Used effectively, such programs enable franchise systems to reach large numbers of potential customers simultaneously. Issues may arise as to the degree of autonomy franchisees have to provide their own unique offers, and what approvals they must obtain from the franchisor. CRM email programs must satisfy a number of legal requirements, including compliance with TCPA and CAN-SPAM requirements, many of which require allowing customers to opt out of offers and other messages received through CRM programs.

Franchisors must consider a variety of factors in selecting services to be included within a mobile app and the timing of the rollout of such services. Franchisors may want to roll out online ordering and payment functions first, followed by such things as CRM, mobile couponing, loyalty, and gift card programs. In some instances, a franchisor and its franchisees may have existing agreements in place with separate vendors for services such as loyalty programs, gift cards, and CRM, and these agreements must be considered when negotiating a development agreement with a mobile app developer and the timing of the rollout of additional services.

C. **Developing a Timeline to Roll Out a Mobile App**

A variety of factors should be considered in developing the timeline for the rollout of a mobile app program. When a mobile app will replace an existing app, the termination and transition processes in the agreement with the current provider will have a major impact on the rollout with the new developer. Mobile app developers must obtain certain information concerning the franchised system and its locations. Such information includes the inventory of products and services available from each location and information on the type of POS system at each location. The rollout timeline must include sufficient time to permit franchisees to disseminate this information to the developer.

Some franchise systems, particularly those with long operating histories, may have widely varying POS systems and technology capabilities in their locations. Franchisees that lack the technology required to implement the mobile app will need sufficient time to acquire, install, and be trained to use the upgraded technology. In developing the implementation timeline, the franchisor will need to allow ample time to test the new app and to train company employees and franchisees in the operation of the new mobile app. Particularly in those systems that are implementing mobile apps and related systems for the first time, rather than replacing or upgrading existing systems, ample time for testing and training may be critical to the success of the rollout.

In planning for the technology upgrades needed for mobile app programs, franchisors will need to review their franchise agreements, franchise disclosure document, and operations manual to confirm that they have the provisions needed to require franchisees to make the required upgrades. As will be discussed in this paper, franchise agreements should have broad and flexible language concerning technology needs, which likely will change significantly during the term of the agreement. As also discussed further below, the franchisor also will need to ensure technology issues are addressed in a number of items in the franchise disclosure.

---

7 The TCPA is The Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227 (2019). Among other things, the TCPA places certain restrictions on commercial text messages. The CAN-SPAM requirements are a reference to the Controlling the Assault of Non-Solicited Pornography and Marketing Act, 15 U.S.C. §§ 7701–7713 (2019), which imposes certain requirements on commercial email messages. These requirements are further discussed in Section VIII.D of this paper.
document. Many of the details of technology upgrades can be addressed in the operations manual, which can be frequently updated to keep up with changing technology requirements.

D. Negotiating Development and License Agreements

After executing appropriate nondisclosure agreements and selecting a mobile app and online ordering developer, the franchisor’s next important task is negotiating the software development and licensing agreement with this developer. The franchisor must balance a complex mix of technological, intellectual property, and contract issues while also being mindful of the needs of three separate groups—the franchisor, its franchisees, and the app developer.

The franchisor and developer may negotiate a master agreement addressing certain general issues, terms, and conditions. The rollout of each product and service, or group of products and services, is then addressed in separate addenda to the master agreement. The master agreement and relevant addenda should (i) describe in sufficient detail the information to be supplied by the franchisor, its franchisees, and the developer, (ii) specifically identify the hardware and software required for all participating locations, (iii) identify the length of the term of the agreement, renewal terms, and the conditions for renewal, (iv) address events of default, whether the defaults are curable, and the time period for curing defaults, and (v) address service level expectations, although these expectations may also be addressed in product or service addenda. These product or service specific addenda also are the appropriate document for describing the testing of products and services before implementation and the timing of the rollout of each product and service. Master agreements for mobile app development or product and service addenda should also address issues found in most technology contracts, including (i) data security and privacy issues, (ii) ownership of data generated by use of the app, (iii) safeguarding the confidential information of the parties, (iv) representations and warranties, (v) exclusivity provisions, and (vi) indemnity and insurance issues.

1. Testing

The franchisor’s obligations to provide access to personnel to work with the developer in creating and rolling out the app should be described in these agreements as well as the franchisor’s obligations to obtain any consents required to include materials within an app or online ordering system. The development of timeframes for testing and rolling out a mobile app is an important issue. Franchisors will want control over who will participate in these tests, but both the developer and the franchisor will want input on the nature and duration of the tests and the results needed to proceed with rollout of the app. Delays in these rollouts are not unusual, and it is important the parties understand who is responsible for certain kinds of delays and the consequences of missed deadlines.

2. Intellectual Property

Protection of the intellectual property of the developer and the franchised system is an important subject to be addressed in the master agreement. The software used to develop a mobile app or online ordering system will often be the developer’s most valuable asset. The developer typically will license certain software used in an app to the franchisor, and will want contractual protections that the client will not attempt to reverse engineer, decompile, or otherwise attempt to use this software for purposes not covered by the development agreement. On the other side, a franchisor will license the developer to use the franchisor’s trademarks, logos, and other intellectual property in developing the mobile app. The franchisor must ensure the parameters of the license granted to the developer are clearly delineated. Typically, both parties
will warrant they have the right to license use of their respective intellectual property and to the best of their knowledge the intellectual property does not infringe on the property of any third party. In negotiating development agreements, a franchisor should keep in mind that it may need to terminate the services of the app developer after the app has been rolled out because the developer is unwilling or unable to perform its ongoing services under its agreements with the franchisor and its franchisees. The franchisor will want to continue to be able to use the software, which it may have paid a substantial amount to have developed for its system. But the developer may be unwilling to permit a third party to maintain the app out of concerns for the confidentiality of its intellectual property. Franchisors should attempt to include provisions in their development agreements making the franchisor the sole owner of all work product in connection with the app. If the developer refuses to agree to this language the franchisor should require language permitting a third party to service the app after a termination in return for compensation to the developer that reflects the value of the developer’s software and non-disclosure protections.

3. **Confidential Information and Trade Secrets**

Not to be overlooked in addressing intellectual property issues is the fact the franchisor will be providing valuable confidential information and trade secrets to the developer. This may include product and service mixes, pricing information, and future product and service development and marketing plans. The franchisor must take all legally required steps to protect these trade secrets to prevent their use for purposes not permitted by the master agreement or product and service addenda. Additionally, the franchisor may have conceived of certain unique features to be included in its app that may include trade secrets or for which the franchisor wants exclusivity for competitive reasons. It is important that such features be addressed in the appropriate agreements to maintain this exclusivity.

4. **Payment Terms**

The master agreement or product and service addenda will include terms for payment by the franchisor and its franchisees. The developer may receive fees that include development fees, per transaction charges for customer use of the mobile app, and monthly charges for various services provided by the developer. Payment terms, remedies in the event of nonpayment, and methods of resolving disputed invoices need to be addressed. The franchisor or its brand marketing fund may pay development fees, but franchisees generally will be responsible for the per transaction charges for their customers and other periodic fees. The franchisor will determine whether its franchisees will deal directly with the app developer for the payment of these charges. If so, the agreements between the developer and franchisor need to make clear that individual franchisees will be solely responsible for payment for charges incurred by the franchisee. As an alternative, franchisees could pay amounts they owe for use of the app to the franchisor, which then pays the developer. Although the franchisor has systems in place for collecting from franchisees, this approach shifts collection risks from the developer to the franchisor. For that reason, franchisors may favor having franchisees contract directly with the app service provider.

---

5. **Legal Compliance**

The master agreement and product and service addenda must address each party’s responsibility for legal compliance. These agreements must allocate responsibility for compliance with the ADA, as discussed in further in Section VII.C., applicable data privacy laws, and laws related to the protection of personally identifiable information.\(^9\) For apps with mobile payment provisions, the parties must address responsibility for compliance with PCI-DSS standards or similar payment security requirements.\(^10\)

6. **Representations and Warranties**

Representations and warranties normally will be included in master agreements and in product and service addenda. They likely will include representations and warranties on the ownership of the parties’ respective intellectual property. A significant part of product and service addenda will be the warranty provided by the developer for a product or service incorporated into the app, along with disclaimers of other express and implied warranties and remedies for breaches of the warranties. Franchisors should be very cautious in permitting developers to disclaim warranties, particularly warranties of non-infringement, because franchisors will want assurances the developer’s software is not subject to claims of infringement by third parties, and the disclaimer of the non-infringement warranty will undercut these assurances. Franchisors should also negotiate for the best possible warranties regarding the proper functioning of the app for its intended purposes, and should seek to limit the developer’s disclaimer of express and implied warranties. These warranties will place the franchisor in a better position to resolve disputes if the app does not function properly when it is rolled out.

7. **Indemnification**

The indemnification section is one of the parties’ most important risk allocation mechanisms in development and licensing agreements. Indemnification and insurance issues are discussed elsewhere in Part IV of this paper. For purposes of negotiating development and licensing agreements, franchisors should be aware of the respective obligations of the developer, franchisors, and franchisees in the development and implementation of mobile app and online ordering programs. Franchisors will want to negotiate strong indemnity obligations requiring developers to indemnify the franchisor and its franchisees from infringement issues related to the developer’s intellectual property and from issues related to the failure of the mobile app to perform in the manner the developer has represented it will perform. Developers will push for indemnification from franchisors related to the franchisor’s intellectual property incorporated into the app as well as protection from claims by third parties against the developer related to the franchisor’s failure to perform its obligations under the development agreement. Both franchisors and developers will want indemnification from franchisees for their failure to follow the terms of agreements entered into by franchisees in rolling out and using the app in their businesses. Franchisors also will want to ensure that their agreements with developers and franchisees provide for indemnification of the franchisor for losses resulting from the failure of the developer

---

\(^9\) The impact of the Americans With Disabilities Act on mobile apps is discussed in Part VII of this paper. For a discussion of the impact of the Act on websites and related issues, see Minh N. Vu and Julia N. Samoff, *Websites, Kiosks, and Other Self-Service Equipment in Franchising: Legal Pitfalls Posed by Title III of the Americans With Disabilities Act*, 36 Franchise L.J. 443 (Winter 2017).

\(^10\) The Payment Card Industry Data Security Standards were developed by major credit card companies to set standards regarding credit card data and reduce fraud. Information on PCI-DSS may be found at www.pcisecuritystandards.org. See Been et al., *supra* note 5, at 33–35.
or franchisees to comply with their obligations to comply with data privacy laws, the ADA, and other laws and regulations addressed in this paper

8. **Defaults**

Franchisors face a number of issues when negotiating contractual provisions concerning defaults under the agreements and the parties’ remedies. Franchisors should be mindful of efforts by developers to limit the developer’s liability and the remedies available to the franchisor and its franchisees for breaches of the development agreement. Franchisors may face significant potential liabilities from consumers and franchisees if issues arise in the rollout and operation of a mobile app and need to ensure the limits of the developer’s liability in the development agreements are commensurate with these risks. Developers also often will seek to have disputes resolved by mediation, arbitration, or litigation in their home state and applying the law of their home state, and franchisors will need to decide if they should push back against these provisions.

9. **Service Level Agreements**

The development agreements between the franchisor and the mobile app developer should address the service level performance requirements the developer will be required to meet. These requirements can focus on the permissible amount of downtime that will occur in the use of the app and the percentages of transactions that must be processed in a timely and accurate manner. Franchisors must ensure that franchisees are aware of these service level performance requirements and that franchisees are familiar with the protocols for reporting service level failures to the franchisor and the app developer. Timely and accurate reporting by franchisees is necessary for the proper functioning of the mobile app and for holding the app developer accountable for the contractually agreed upon performance requirements.

10. **Exclusivity**

App developers may seek to include terms in the development agreement making the developer the exclusive mobile app vendor for the system. Developers may assert that this is necessary to enable them to recoup their upfront costs in developing and rolling out the app. Franchisors may agree to exclusivity to receive more favorable pricing. But, in doing so, franchisors should be aware of any unique requirements or aspects of a franchisee’s operation that may make it more difficult for that franchisee to implement the developer’s app. It may be necessary for franchisors to negotiate limited carve-outs from the exclusivity provisions to address unique or unusual situations.

11. **Termination and Expiration**

In negotiating agreements with app developers, franchisors should consider the rights and obligations of the parties upon termination or expiration of a development or license agreement. Given the importance of having a mobile app and online ordering for many franchised systems, it is important for the franchisor to negotiate terms providing for reasonable levels of cooperation by the developer in transitioning the system to a new mobile app and online ordering system. A clear understanding of what aspects of the technology of an app may be used by a franchised system in the future will make it easier to negotiate details of a transition.

In summary, in negotiating agreements with app developers franchisors face the difficult task of balancing the objectives of the franchisor, its franchisees, and the app developer. Franchisors should consider focusing on these issues: (i) hardware and software requirements
to implement the app and their cost; (ii) time frames for developing and rolling out the app and consequences for failure to meet these time frames; (iii) cybersecurity issues; (iv) the scope of the training to be provided by the franchisor, its franchisees, and the developer; (v) information to be provided to developers and protecting confidentiality and intellectual property rights of this information; (vi) the length of the term of agreements with developers, renewal, and termination; and (vii) indemnity and insurance issues.

E. Integration of Apps with POS Systems

In planning for the implementation of a mobile app and online ordering into a franchised system, the franchisor will need to determine whether use of the app will be integrated into the POS systems used by the franchisor and franchisees at their locations. Integrating the app with POS systems can help streamline the mobile app online ordering process with significant customer service benefits, but can introduce an added level of complication into the rollout of the app and online ordering system. When most of the franchised system operates using similar POS systems, rolling out the app on an integrated basis may be realistic. However, if a system has a variety of different POS systems, a rollout of a mobile app on a non-integrated basis may be more feasible with integration to the POS system to follow at a later time. In some cases, franchisors may be able to use their POS vendor to develop a mobile app, but if that is not the case, the development of an app integrated with POS systems will require cooperation between the app developer and the POS system provider. This can add yet another layer of complexity to the app development and rollout process.

Requiring franchisees to make major hardware and software upgrades, including upgrades to the POS system, to participate in a mobile app program may make it more difficult for the franchisor to convince franchisees of the merits of implementing a mobile app program, particularly when the franchise agreement is not clear on the franchisor’s ability to require franchisee participation in the app program. This requires the franchisor, and perhaps its franchisee advisory groups, to sell the merits of the program to reluctant franchisees. They may need to be convinced that customers will likely continue to demand the additional convenience and services provided by mobile apps, and implementing the program will provide significant marketing opportunities for franchisees as well as access to valuable additional information concerning customers and their preferences.

F. Terms and Conditions of Use

In rolling out its mobile app a franchisor will need to prepare a well-drafted set of terms and conditions regarding the use of the app by consumers. The developer also will need to be involved in preparing these terms and conditions. In some cases, the developer will be the licensor under what is sometimes referred to as an End User License Agreement (EULA). These EULAs normally will contain terms limiting the liability of the developer, the franchisor, and franchisees, and prohibiting consumers from attempting to decompile, reverse engineer, or use the mobile app software for other than its intended purpose. EULAs also may contain mandatory arbitration provisions, including waivers of class arbitrations. Customers should be required to consent to the EULA when they download the app, so the app will need to provide a link to the EULA to enable customers to review it. The app should also provide a link to the franchisor’s privacy policy in light of the amount of customer data the app will collect.
G. Integration of Mobile Apps with Social Media Sites

Most franchised systems maintain an active presence on social media sites. Franchisors will want to ensure their mobile app can readily interface with sites such as Facebook, Twitter, Instagram, and Snapchat to enhance the experience of app users. Among other things, this interface will require the franchised system to comply with the terms and conditions mandated by the social media platforms.

Integration with social media sites can improve the functionality of mobile apps in a number of ways. If a franchisor has its social media feeds for sites such as Facebook, Twitter, and Instagram placed within its app, this enables users of the app to learn about offers, events, and other information regarding a franchised system found on social media without leaving the app. Integration of an app with social media sites also provides a franchisor and its franchisees with valuable information on the preferences, likes, and dislikes of its customers, further enhancing the ability of franchised businesses to target offers to specific customers. App users can share their experiences with franchised locations on social media, thereby increasing the system’s visibility, without leaving the app. The ability to access social media sites through the app provides consumers more incentives to use the app. Allowing users to log into the app through Facebook or other social media sites provides easier access to the app, and its online ordering capabilities, because users do not have to log into the app separately. The huge number of consumers with social media accounts provides greater visibility for an app that is well-integrated into social media sites.11

III. DATA PRIVACY CONCERNS

The interest in privacy is longstanding. The principle that protects personal writings and any other productions of the intellect or of the emotions is the right to privacy, and the law has no new principle to formulate when it extends this protection to the personal appearance, sayings, acts, and to personal relation, domestic or otherwise.12 This interest has led to statutes and regulations that protect privacy, including the Health Insurance Portability and Accountability Act (HIPAA), the Children’s Online Privacy Protection Act (COPPA), and the Fair Credit Reporting Act (FCRA).13

Franchises developing mobile apps need to keep privacy considerations at the fore, especially in light of recent legislation in this area—the European Union’s General Data Protection Regulation (GDPR) and the California Consumer Privacy Act of 2018 (CCPA).

A. Application of Data Privacy Statutes and Regulations

Various data privacy statutes and regulations affect a franchise’s development and use of mobile apps. This is an area of legislation that is continually developing. Two recent developments in legislation, as mentioned above, are the GDPR and the CCPA. Additional developments that specifically affect mobile apps are likely in the future. As an example, the

---

The APPS Act of 2018 was introduced in Congress in July 2018. The purpose of the APPS Act is “[t]o provide for greater transparency in and user control over the treatment of data collected by mobile applications and to enhance the security of such data.” While the act has not proceeded further, it is not hard to imagine it becoming law.

1. The GDPR

The GDPR became effective May 25, 2018, and has broad application.

The GDPR not only applies to organizations located within the EU but also applies to organizations located outside of the EU if they offer goods or services to, or monitor the behavior of, EU data subjects. It applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company’s location. In short, even franchisors based in the United States need to consider whether the GDPR applies to their mobile apps.

The goal of the GDPR is to “protect all EU citizens from privacy and data breaches in today’s data-driven world.” The GDPR endeavors to achieve this goal through the following mechanisms:

- Mandatory data-breach notifications;
- Right of “data subjects” to know whether their personal information is being processed;
- Right of “data subjects” to have their personal information erased;
- Right of “data subjects” to receive their personal information from one “data controller” and send it to another “data controller”;
- Requiring the design of systems to include privacy considerations from the beginning of the design process;
- Requiring Data Protection Officers (DPOs) and internal record keeping standards; and
- Enforcing these provisions through tiered penalties and a private right of action.

“Personal information” is intended to be broad and includes any information that can identify a person.

Franchises with business interests or connections in the European Union need to be aware of the GDPR and take action to comply with its requirements. Generally, this will involve providing information to people about the personal information collected about them and giving them the ability to control their personal information. More particularly, to ensure compliance with the GDPR, businesses will need to develop practices and policies for keeping track of the personal

---

15 Id. Previous versions of the APPS Act were introduced in 2013 and 2016.
17 Id.
19 Id.
20 EU GDPR.ORG, supra note 16.
information they gather so that they can more efficiently respond to consumers’ requests relating to their personal information. One manner in which businesses could accomplish this is to create an inventory of personal information organized by each consumer. This approach would enable a business receiving a request from a consumer to efficiently locate and take follow-up action relating to that request—for example, deleting the consumer’s information.

Franchises need to keep in mind that violations of the GDPR can bring hefty fines, up to “4% of annual global turnover […] or €20 million,”21 This is the maximum possible fine, and the GDPR does utilize a tiered penalty approach. Nevertheless, violations of the GDPR can bring serious financial consequences.

2. The CCPA

The CCPA provides people similar rights as the GDPR, including the right to know what personal information is collected about them, the right to have businesses not sell their personal information, and the right to have businesses erase their personal information.22 As in the GDPR, “personal information” is broadly defined to include any identifying information.23

The CCPA goes into effect on January 1, 2020,24 and generally applies to for-profit businesses that collect personal information of California residents, conduct business in California, and have overall gross revenues that exceed $25 million (including revenues generated inside and outside California), or conduct a certain amount of business involving the personal information of California residents.25

Like the GDPR, enforcement of the CCPA will be accomplished through imposition of fines for violations and litigation exposure.26 More particularly, fines range from $2,500 for unintentional violations of the CCPA to $7,500 for intentional violations of the CCPA.27 In addition, the CCPA provides a private right of action to consumers in the event of a data breach.28

For fines imposed relating to violations of the GDPR and the CCPA, the franchisor needs to consider including indemnification provisions in the franchise agreement that allocate the cost of those fines to the franchisee, if the franchisee’s conduct led to the imposition of the fines. While the franchisor will be more likely to be responsible for responding to requests relating to personal information, it is possible for franchisee conduct—such as misuse of consumer personal information—to lead to fines under the GDPR or CCPA. In those instances, the franchise agreement should require that the franchisee indemnify the franchisor for those fines.

21 EU GDPR.ORG, supra note 16.
24 Id. at 27.
25 Id. at 29.
26 Id. at 28.
27 Id.
28 Id.
Similar to compliance with the GDPR, franchises with business interests or connections in California need to be aware of the CCPA and take action to comply with its requirements. As with the GDPR this will include providing people with information about the personal information collected about them and giving them the ability to control their personal information. Again, organization will be the key to ensuring a franchise can efficiently comply with requests from consumers to access their information or erase their information. Creating an inventory of personal information organized by consumer, as described above, could facilitate compliance with the CCPA.

Further, other states could soon follow California’s lead and adopt legislation similar to the CCPA. As a result, developing policies and procedures to comply with the CCPA should help businesses be prepared to comply with potential future privacy regulations adopted by other states.

B. Issues Related to Mobile Pay Functions in App

Another consideration for a franchise developing a mobile app is whether to include functionality that allows a customer to make purchases within the mobile app. Including this functionality can enable customers to more easily make purchases of goods or services offered by the franchise. However, including this functionality requires franchises to be aware of certain statutes and regulations, including the Electronic Funds Transfer Act (EFTA), the Gramm-Leach-Bliley Act (GLBA), and the Bank Secrecy Act (BSA).\(^9\) These laws were not drafted with mobile apps in mind; however, portions of the laws were drafted broadly enough to encompass payment functionality in mobile apps, which requires a franchise brand to pay attention.

Generally, the EFTA limits consumers’ liability in connection with fraudulent activity in their accounts—for example, limiting a consumer’s liability for fraudulent spending on their debit card account if they timely report the debit card as lost.\(^{30}\) The EFTA also requires a business to disclose certain information to consumers, including the business’s confidentiality terms.\(^{31}\) The GLBA also requires certain disclosures and protection of consumers’ financial information: “The GLBA requires financial institutions to explain their information-sharing practices to their customers as well as safeguard sensitive data.”\(^{32}\) The BSA requires financial institutions to provide certain information to authorities for use in investigations, including criminal investigations.\(^{33}\) In other words, it is an act that can be implicated after a crime has occurred and the authorities seek access to financial information.

Depending on the particular features of mobile apps, including in-app payment features, franchisors will need to review the applicability of the provisions of the EFTA, the GLBA, and the BSA. As an example, a franchisor developing a mobile app with in-app payment functionality could fall within the scope of the EFTA and be required to limit a customer’s liability for fraudulent in-app purchases. Failure to do so could result in violation of the EFTA.


\(^31\) Gregson, supra note 29, at 323.


Finally, given the relative newness of mobile apps and in-app purchases more particularly, franchisors developing and using mobile apps with in-app purchase functionality will need to keep current on developments in applicable statutes and regulations, which developments will likely accompany developments in in-app purchase technology and the growing use of such technology.

C. Issues Concerning Data Privacy Breaches

Breaches of data privacy occur with some regularity. A business, including a franchisor, that develops and uses a mobile app needs to prepare for the possibility of a data privacy breach that reveals customers’ personal information. Such an event could have damaging effects, including negative publicity, customer distrust, and litigation exposure.

A franchisor developing a mobile app needs to put measures in place to prevent a data breach. This is expressly required by the GDPR and encouraged by the private right of action created by the CCPA. Anti-breach measures, such as more robust security for the app, will certainly help prevent a data breach in the first place. And, if a data breach occurs despite a business’s implementation of anti-breach measures, these measures could also help defend against post-breach issues such as negative publicity and litigation.

If a data breach does occur, the GDPR requires that the business that experienced the breach notify consumers. In addition to being required, notification, like preventative measures, could help defend against negative publicity and litigation. A franchise should prepare to take a unified approach to dealing with a breach. This can be difficult given the franchise model, but it will be essential to handling the breach efficiently and effectively.

If a data breach occurs it is critically important that franchisees understand their responsibility to report such breaches to the franchisor. Data breach laws in every state require a variety of responses following a breach. Although similar in nature, state laws vary as to the actions companies must take after learning of a data breach and the time-frames for notifying affected consumers also vary. These responses may include required reporting to governmental agencies, notification to customers whose data has been breached, and in some cases the operators of company-owned and franchised locations may be required to offer free credit monitoring services to customers affected by the breach. It is important that franchisors have strong language in their franchise agreements, operations manuals, and technology and social media policies requiring franchisees promptly to comply with all data breach reporting and responses requirements and cooperate with the franchisor in its compliance with these requirements.

D. The Relationship Between Terms and Conditions for Use and Data Privacy Issues

As discussed above, some data privacy statutes and regulations, as well as some statutes and regulations that govern mobile app payments, require disclosure of certain information to consumers. As a result, a franchisor developing a mobile app needs to consider these disclosure requirements and determine what information needs to be disclosed in the terms and conditions for the mobile app.

As an example, the CCPA requires a business to disclose to consumers information about the categories of personal information collected about the consumer, as well as the intended use
of each such category of personal information. To the extent a mobile app collects personal information, the terms and conditions for the mobile app will need to include this required disclosure information, if the CCPA applies.

What information the terms and conditions for a mobile app will need to contain will depend on what privacy statutes and regulations apply to the mobile app, what information the mobile app collects, and what features the mobile app includes.

E. Ownership of the Data Collected in Apps

A central feature of both the GDPR and the CCPA is to give consumers control over their personal information. For example, both the GDPR and the CCPA contain provisions requiring a business to delete a consumer’s personal information in certain circumstances. Further, both the GDPR and the CCPA allow consumers to opt-out of having their personal information sold.

Clearly, there is a value to user data, and franchises can benefit from collecting such data. Nevertheless, a franchisor developing and using a mobile app that collects personal information needs to be aware of the rights the GDPR and the CCPA give consumers over their personal information and be ready to respond to consumer requests relating to their personal information. If the GDPR and the CCPA are applicable, a franchisor cannot ignore consumer requests relating to personal information on the basis that the franchise collected the personal information through its mobile app and now owns the information. Proactively developing an organized system to track and maintain user data will be essential to responding to consumer requests. This is more an operational issue than a legal issue. Nevertheless, the GDPR and the CCPA make clear that a company collecting consumer information needs to be ready to respond to those requests, and efficiently maintaining that information will put a company (including a franchise company) in the best position to respond to those requests.

IV. INSURANCE ISSUES

Another consideration in developing a mobile app is appropriate insurance coverage. This includes not only the coverage carried by the franchisor, but also the coverage carried by those involved with development of the mobile app and the coverage carried by the franchisees. In general, it is important to ensure that coverage is in place for the more common and costly risks associated with mobile apps.

The obvious frontrunner of such risks is a data breach. This, too, is a relatively new and developing area with little standardization of terms and language: “The cyber insurance market is a virtual wild west of insurance policies with no standardization of coverage or policy language, which makes it almost impossible to compare policy pricing and coverage.”

34 See supra Part III(A)(2).
35 See supra Part III(A)(1)-(2).
A franchisor needs to consider what insurance coverage is necessary to cover losses related to the mobile app. This should include coverage for the franchisor, the entities involved with the development of the mobile app, and the franchisees.

A franchisor should arrange coverage for losses it may sustain in the event of a cyber-attack such as hacking or a data breach. These losses could include the costs to notify customers of the data breach, legal costs, and lost profits while dealing with the cyber-attack. A franchisor should also consider coverage for third-party losses. These losses could include liability to third parties for personal information accessed during a data breach or losses associated with fines and penalties related to the data breach.

A franchisor developing a mobile app should ensure that the entities involved with the development of the app have insurance coverage in place to cover data security breaches caused by errors in the development of the app. For example, if vulnerability in the design of the mobile app results in a data breach, the franchisor may want to hold the entity responsible for the vulnerability accountable, and if that entity has insurance coverage for such an event, it may help the franchisor cover its losses resulting from the data breach. Relatedly, the franchisor may want to include indemnification provisions in its contracts with the entities involved in developing its mobile app that would require those entities to hold harmless the franchisor in the event their error in the design or construction of the mobile app leads to a data breach and losses for the franchisor.

While franchisees likely will have less involvement with the development and maintenance of a mobile app, franchisors and franchisees should ensure that franchisees have insurance coverage for risks associated with their use of the mobile app to the extent reasonably possible. Given that franchisees will be the ones interfacing with customers and interacting with the app and information gathered by the app on a daily basis, franchisees could have particular risks associated with data breaches and misuse of customer information. The impacts of such risks, if realized, could include lost profits while dealing with a data breach, costs associated with dealing with a data breach, and, potentially, liability to third parties related to the data breach. And, as with indemnification considerations between the franchisor and the app developers, the franchisor and franchisee should consider including in the franchise agreement indemnification provisions relating to losses resulting from mobile app data breaches. Such provisions will be especially important if it was the franchisee’s conduct that led to the breach.

V. ROLLOUT AND COMMUNICATION OF BENEFITS TO FRANCHISEES

An important point for a franchisor to consider is how it will manage the rollout of the mobile app to its franchisees. Careful planning and execution of the mobile app rollout can go a long way in helping to ensure that the franchise system is prepared for the launch of the mobile app program and contribute to the overall success of the program. Franchisors will want to ensure that franchisees have readily available access to the knowledge and equipment necessary to participate successfully in the mobile app program. Franchisors should be clear in their communications about their expectations for the program, the requirements of franchisees, the timeline for rollout, and instructions for participating in the program.

37 Id.
38 Id.
A. Determine Required Technology Updates for Franchisee Participation in Mobile App Program

Early on in the development of the mobile app program, franchisors will want to consider any technology updates that will be necessary in order for franchisees to participate in the mobile app program. As part of this process, franchisors will want to review the hardware and software that are currently in use by franchisees, and evaluate whether the franchisees will need to make additional purchases in order to receive orders from the mobile app, honor mobile app coupons, process loyalty transactions, or to carry out any other functions necessary to participate in the mobile app program. For example, if the redemption of mobile app coupons or the processing of loyalty transactions will require the scanning of a barcode or QR code, franchisors should consider whether franchisees will need to purchase scanners or will the coupons or loyalty cards be read by equipment that is already in use at the franchise locations. To the extent that franchisees need to acquire new equipment in order to participate in the mobile app program, the franchisor should set specifications for the necessary equipment and decide whether franchisees can source their own equipment, so long as it meets specifications, or if the franchisees will be required to purchase specific equipment from a specific vendor. In addition, franchisors will also want to evaluate whether the mobile app will integrate with the POS that is currently in use by franchisees, or will software updates be required. If franchisees will need to acquire a license to specific software in order to integrate with the mobile app, franchisors should evaluate whether it makes sense for the franchisees to license the software directly from the vendor or for the franchisor to acquire a license from the vendor that allows it to sublicense to franchisees.

B. Scope the Cost for Franchisees to Implement Mobile App Program

The cost to implement the mobile app program will likely be an important factor to franchisees in their decision to participate, to the extent that it is voluntary, and franchisees' acceptance of the franchisor's decision to roll out a mobile app program. In particular, franchisees will be interested in the cost of participation versus the anticipated benefit of having a mobile app program. Some costs to consider are any equipment purchases the franchisee will need to make, as well as any software purchases or ongoing licensing fees that will be paid by the franchisee. Franchisors may want to evaluate ways to reduce technology costs placed upon participating franchisees through programs such as equipment leasing. Franchisors should also contemplate other less tangible costs to franchisees, such as increased labor and insurance costs if, for example, franchisees will need to hire additional employees to process orders or franchisee employees will be delivering orders placed through the mobile app. Another potential cost to franchisees is the cost associated with any product or service discounts provided to customers in connection with the mobile app. If the mobile app has a loyalty component, franchisors should consider who will bear the cost of goods for transactions that are processed using loyalty points. Will the cost be borne by the franchisee who is processing the loyalty redemption, will a pool of funds be created to credit franchisees, and will any portion of the cost be covered by advertising funds or royalties? In some instances, there may be cost savings to franchisees through operational efficiencies that are created by the mobile app, which defray the cost of implementation. Franchisors may also want to evaluate other ways in which it might defray the cost of implementation to the franchisees; for instance are there vendor incentives or will any of the implementation cost be covered by technology fees, royalties, or advertising fees that the franchisees are already paying? In some instances, the franchisor may offer incentives, such as royalty credits, to encourage franchisees to participate in the mobile app program.
C. Determine If Program Is Voluntary Or Mandatory

Franchisors will also need to determine whether franchisee participation in the mobile app program will be voluntary or mandatory. If the franchisor is considering making participation mandatory, it should carefully review its franchise agreement and what the franchisor has disclosed in its Franchise Disclosure Documents (FDDs), as discussed further below, to ensure that it can require franchisees to participate without incurring liability. On the one hand, mandatory participation may be desirable to customers, as they will not need to identify which locations are participating in the program or travel to a farther location in order to utilize the mobile app. In addition, mandatory participation could avoid the loss of customers of one franchisee to another due to one location participating in the mobile app program while the other location is not. Franchisors should also consider any supply cost savings that might be achieved if participation in the program is mandatory. On the other hand, franchisors will also want to consider the benefits of making participation in the mobile app program voluntary. Franchisors should evaluate how many franchisee locations are currently equipped to participate in the mobile app program, as well as the costs of franchisees to implement the program. Franchisors may also want to consider franchisee willingness to participate in the mobile app program and anticipated customer adoption. Another factor to contemplate is how the franchisor will monitor participation in the program if participation is mandatory and the cost of enforcement by the franchisor. If possible, franchisors might consider testing the program in a few locations and/or making participation in the program voluntary when the program is first rolled out. This could allow for franchisors and franchisees to evaluate the program and make any necessary modifications before the costs associated with system-wide adoption of the program are incurred. Furthermore, it may be beneficial for the franchisor to facilitate a committee of franchisees that are testing the program or are early adopters of the program, in order to receive franchisee feedback and to foster franchisee buy-in.

D. Franchise Disclosure Implications

Franchisors should think about any portions of their franchise disclosure documents that will need to be updated to reflect the implementation of the mobile app program. The Federal Trade Commission Rule on Franchising (FTC Rule) requires that a number of items in the franchise disclosure document address issues relevant to the rollout of a mobile app program. Any technology fees charged by the franchisor will need to be discussed in Item 6 of the FDD and may need to be described in a footnote to that Item. Furthermore, the costs of any equipment, software, and other items related to the implementation of the mobile app must be disclosed in Item 7 of the FDD as an expense of opening a franchise outlet. The cost should also be included in the total estimated initial investment that is stated on the FDD cover page. Furthermore, if the Franchisor will be selling or providing equipment to franchisees that should be disclosed in Item 5 of the FDD and on the FDD cover page.

The FTC Rule requires disclosure in Item 8 of the franchise disclosure document of certain specific information concerning a franchisee’s obligations to purchase computer hardware and software. This will require disclosure of the hardware and software a new franchisee must purchase in connection with implementing the franchisor’s mobile app program and online

41 16 C.F.R. § 436.5(e) (2019).
The information provided in this disclosure should include whether this hardware and software must be purchased from the franchisor or sources designated or approved by the franchisor or if the franchisee chosen vendor must meet specific requirements, as well as disclosure of any ownership interest the franchisor or its officers have in any company from which the franchisees are required to make these purchases. Furthermore, any franchisee obligations with respect to the mobile app program, whether under the franchise agreement or other agreements, should be disclosed in Item 9 of the FDD. If any financing will be offered in connection with the mobile app program, including any franchisor equipment leasing programs, their existence as well as the associated terms and requirements should be disclosed in Item 10 of the FDD.

Item 11 of the FTC Rule requires the franchisor to disclose “whether the franchisor requires the franchisee to buy or use electronic cash register or computer systems.” Any computer systems the franchisee is required to use in connection with the mobile app program should be disclosed in Item 11. The FTC Rule also requires the disclosure of information including the types of data to be generated, the initial and ongoing costs of the system, any obligation of the franchisor to provide ongoing maintenance or related services, and whether the franchisor will have independent access to the information to be stored on the franchisee’s system. Franchisors should also consider whether any assistance or training they provide to franchisees in connection with the mobile app or any allocation of advertising funds to the mobile app program also needs to be disclosed in Item 11.

If franchisees will have a territory associated with mobile orders, franchisors should consider whether that needs to be disclosed in Item 12 of their FDD. If the franchisor has any patents, copyrights, or proprietary rights in any elements of the mobile app program, those should be disclosed in Item 14 of the FDD. It may also be appropriate for the franchisor to disclose in Item 15 of the FDD any restrictions on the number of franchisees on a particular franchise agreement that can be a party to a EULA for required software, as this may impact the franchisee’s obligation to participate in the franchise business. In addition, any contracts that the franchisee may enter into in connection with the mobile app program should be disclosed in Item 22 of the FDD and should be provided as exhibits to the FDD. Franchisors should be mindful that other areas of the FDD may be affected depending on the nature of the mobile app program, and should review accordingly.

E. Timeline For Franchisee Rollout

When thinking about the timing of the mobile app program rollout, there are several factors the franchisor may want to assess. A franchisor may want to consider what its competitors are
doing and any market studies showing how likely its customers are to use the mobile app and the potential impact on sales. Indicators of a strong need for the mobile app in order to stay competitive, and/or a significant impact on franchisee sales, might drive a quicker rollout to the franchise system. However, there are additional considerations that may impact the timeline. Franchisors will want to consider how long it will take to source vendors and enter into the appropriate contracts, if it has not done so already. Franchisors will also want to determine how long it will take franchisees to acquire the equipment and software necessary to participate in the mobile app program and to implement any necessary operational changes. Another factor to consider is the schedule for franchisee training and the timeframe for franchisees to train their employees. Franchisors may find that it would be beneficial to stagger the rollout of the program in order to better manage the implementation and may choose to identify specific franchisees based on their capabilities or willingness to participate. They may also choose to roll out the program on a geographic basis.

Aside from considering the time that it may take for franchisees to get up and running to be able to use the mobile app program, franchisors may want to take into account time of year and additional operational and marketing considerations. For example, the busiest times of the year according to sales volumes may or may not be the best time to roll out the mobile app program. Franchisors may also want to consider how marketing and advertising initiatives will coincide with the mobile app rollout.

F. Training for Franchisees

Careful attention to franchisee training can contribute to a smoother rollout of the mobile app program. Franchisors should consider the best means to provide training to franchisees in order for them to adequately understand how to process transactions made using the mobile app and how to implement any related operational changes. For example, if franchisees will need to make operational changes in order to implement a quick pick up process for mobile orders, franchisees should be trained on how to modify their existing operational procedures. Additional training aspects to evaluate are whether any training will be provided to the franchisees or their employees by the vendor, the format of the training (i.e., classroom, web-based, etc.), and the location of the training. When developing training, franchisors should keep in mind that franchisees will likely need to provide the same or similar training to their employees and that franchisees may face their own training challenges, such as employee schedules and busy shifts. Training should be created with the goal of facilitating franchisees in being able to ensure that they and their employees are ready to process customer transactions through the mobile app when it is implemented at their location. Failures in training could have a negative impact on customer experience and customer willingness to adopt the mobile app program as part of their purchasing experience.

VI. FRANCHISEE COMPLIANCE WITH MOBILE APP PROGRAM REQUIREMENTS

A. Defining Participation Requirements

As discussed in this paper, the development and implementation of a mobile app and online ordering into a franchised system involves a complex set of interactions involving the app developer, the franchisor, and franchisees of the system. The first issue for the franchisor is whether franchisee participation will be voluntary or mandatory. The importance of uniformity in a franchise system will argue for mandatory participation, but poor technology skills or deficiencies in operations may argue in favor of excluding some franchisees, at least initially.
It is important that franchisors clearly communicate to their franchisees the requirements and expectations for franchisee participation in the mobile app program. Franchisors will want to delineate the hardware and software upgrades that will be required to participate in the program and the timeline for these upgrades, mandate that franchisees must be in compliance with their franchise agreements when they implement the mobile app program, ensure that franchisees have signed all documents required by the app developer, and ensure that franchisees understand the training their personnel must complete before rolling out the app.

B. Sources of Mobile App Program Requirements

Franchisors face many challenges when addressing technology issues in drafting franchise agreements. Available technologies change rapidly over short time periods, which can conflict with the long-term nature of many franchise agreements. For this reason, franchisors may want to address technology requirements only in general terms in the franchise agreement. Franchisors should reserve the right to implement and require franchisees to implement new technologies designed to improve franchisee operating results and stay ahead of competitors in adapting these technologies. The franchise agreement should be clear that the implementation of new technologies may require significant capital expenditures.

The specifics for implementing a mobile app program may be addressed in the operations manual or separate communications from the franchisor. The franchisor should address the hardware and software upgrades required to implement the mobile app program along with the information on approved or required vendors. The franchisor should address in detail the timeline for the rollout of the app to franchisees, including a description of the required training on the use of the mobile app. Franchisors should also consider how they will enforce franchisee obligations and how they will evaluate franchisee compliance.

C. Agreements between Franchisees and the App Developer

Franchisees may also need to enter into a contractual relationship with the app developer. This contract should address such topics as the products and services provided to the franchisee through the app, the fees to be charged to franchisees, the terms for payment, and the duration of the agreement. This agreement also will include a list of the franchisee’s locations. Franchisors will want to provide that franchisees are solely responsible for the charges they incur with the developer in using the mobile app, and that the franchisor is not responsible if a franchisee does not pay for the developer’s services in a timely manner.

Developers may want franchisees to be responsible for agreeing to a number of terms the developer negotiated with the franchisor. These terms may include restrictions on how the developer’s software can be used, limitations of liability, and disclaimers of certain representations and warranties. Rather than describing these provisions in detail in the agreement with franchisees, app developers may instead choose to incorporate these terms by reference into their agreements with franchisees. This requires the franchisor to carefully consider the terms

---

51 The importance of clear language in the franchise agreement on technology matters is illustrated in Bores v. Domino’s Pizza LLC, 489 F. Supp. 2d 940 (D. Minn. 2007), rev’d, 530 F.3d 671 (8th Cir. 2008). In Bores the issue was whether the language in the franchise agreement permitted Domino’s to both provide specifications for a new computer system and specify sole approved vendors. Id. A decision in favor of the franchisee by the trial court was reversed by the Eighth Circuit, but the dispute over the franchise agreement language delayed implementation of the new system.
that should be incorporated into agreements with franchisees and those terms that should not be incorporated.

**D. Impact on Franchise Agreement and Other Documents**

The implementation of a mobile app program within a franchised system will likely require additional disclosures in a franchisor’s franchise disclosure document, franchise agreement, and related documents. The rapidly changing technology environment in which franchise systems operate makes it advisable to address technology issues only in general terms in the franchise agreement. This language should make it clear that the franchisor has the right to introduce new technologies, such as a brand-specific mobile app, into the system and to require franchisees to implement these new technologies even when implementing such technologies will require additional capital expenditures by franchisees. The details regarding the forms of technology to be introduced into the system and such matters as the hardware and software requirements and required training can be addressed in operations manuals and other communications by the franchisor to the franchised system.

Franchisors should consider whether to put the terms and conditions of a mobile app rollout into an amendment to the franchise agreement, or possibly into a stand-alone document. Clearly describing the implementation requirements in a document signed by franchisees will make it easier for the franchisor to take action if a franchisee fails to satisfy these requirements. If these requirements are in an amendment to the franchise agreement, the franchisor can exercise the remedies for default in the franchise agreement if the franchisee materially breaches these requirements.

**E. Prohibitions on Use of Unapproved Technology**

The system wide integration of a mobile app program can be integral to the program’s success. This makes it important for the franchisor to have strong language prohibiting the use by franchisees of any unapproved technology, including mobile apps. This language should appear in the franchise agreement and be strictly enforced by the franchisor. The use of unapproved mobile apps can create customer confusion and can increase the franchisor’s risk including cyber liability risks.

**VII. ADA COMPLIANCE ISSUES**

In evaluating legal risk associated with a mobile app program, franchisors should carefully consider the impact of the ADA. The number of lawsuits filed each year claiming violations of inaccessible websites, including mobile apps, has increased significantly. In 2018 alone, the number of ADA lawsuits filed federally tripled from the prior year, with approximately 814 ADA web accessibility lawsuits being filed in 2017 and approximately 2,258 filed in 2018.

---

52 Issues concerning additional disclosures in franchise disclosure documents are discussed in Section V.D of this paper.

Title III of the ADA prohibits discrimination on the basis of disability in places of public accommodation. A public accommodation is defined in the ADA as a privately operated facility affecting commerce that falls into one of twelve categories: places of lodging, establishments serving food or drink, places of public gathering, sales or rental establishments, service establishments, public transportation terminals, depots, or stations, places of public display or collection, places of recreation, places of education, social service center establishments, or places of exercise or recreation. Private clubs and establishments and religious organizations are exempt from the requirements of Title III. Title III provides a private right of action, allowing individuals with disabilities to seek injunctive relief and attorney’s fees, but not damages. However, plaintiffs may seek damages through certain state or municipal laws that parallel the ADA. For example, under California’s Unruh Civil Rights Act, a violation of the ADA is also a violation of Unruh and provides for a minimum of $4,000 in damages for a violation of Unruh. In addition, the US Attorney General has the option to join an ADA suit and seek additional monetary relief to the plaintiff.

A. Application of the ADA to Mobile Apps

The ADA does not expressly limit its coverage to brick and mortar establishments. However, it does not specifically state that its coverage extends to beyond brick and mortar establishments either. The ADA’s silence with respect to virtual spaces is likely to due to the minimal use of the Internet when the ADA was enacted in 1990. The U.S. Department of Justice (DOJ), which is charged with enforcing the ADA, has taken the stance that the websites and mobile apps of public accommodations are within the scope of the ADA. The lack of reference to websites and mobile apps in the text of the ADA has not stopped the DOJ from taking enforcement action against private companies whose websites and mobile apps are not accessible to disabled individuals. This is evidenced by the 2014 settlement agreement that it entered into with Peapod, LLC and the consent decree that it entered into with H&R Block, both of which required the companies to remedy ADA violations on their websites. The Peapod, LLC settlement agreement specifically addressed mobile apps. Notably, the

---

55 Id. at § 36.104 (2019).
56 Id.
57 CAL. CIV. CODE § 51 (West) (2019).
58 CAL. CIV. CODE § 52 (West) (2019).
60 Elizabeth Bowersox, McAfee & Taft, DOJ Confirms Websites are Covered by ADA, but Offers Some Flexibility to Businesses in Complying, JDSUPRA (Oct. 26, 2018), https://www.jdsupra.com/legalnews/doj-confirms-websites-are-covered-by-56505/.
Peapod, LLC settlement agreement by and large requires Peapod to take the same actions to provide accessibility on its mobile app as it is required to take with respect to its website.63

In addition to enforcement action by the DOJ, an increasing number of ADA lawsuits are being filed by disabled individuals against companies for allegedly inaccessible websites and mobile apps. The courts have been split on whether the scope of the ADA is limited only to businesses with a physical footprint or whether it reaches businesses that solely have a digital presence. The First, Second, and Seventh Circuits have found that a website can be a place of public accommodation without the need for a connection to a physical premises.64 However, the Third, Sixth, Ninth, and Eleventh Circuits have concluded that places of public accommodation must be physical spaces; goods and services provided by the public accommodation, for example mobile apps, could fall within the scope of the ADA if they have a sufficient nexus to the physical location.65

There have been a number of ADA lawsuits specifically addressing the accessibility of mobile apps of public accommodations.66 The plaintiffs who bring these lawsuits generally allege that they are disabled individuals who are unable to use features of the mobile app because the business has failed to implement features to make the app accessible to disabled individuals, and therefore have discriminated against disabled individuals by denying them access to the business' goods and services.67 For example in Farmer v. Sweetgreen, claims were asserted relating to Sweetgreen’s mobile app, and the plaintiffs cited Sweetgreen’s marketing of its online ordering portal and mobile app as a fast and efficient way to order food for pick up upon arrival at the restaurant, in further support of its discrimination claims.68 In other words, the alleged inaccessibility of the mobile app to certain individuals with disabilities makes it so that only individuals without these disabilities can access the faster and more efficient services offered by the business. Plaintiffs and courts have analyzed the application of the ADA to mobile apps of public accommodations in the same way that they have analyzed the application of the ADA to websites of public accommodations. These matters are often resolved by settlement with the defendants agreeing to bring their mobile apps into conformance with an agreed up accessibility standard by a specific date.69

63 U.S. Dept. of Justice, supra note 61.
64 Title III of the Americans with Disabilities Act (ADA): Website Compliance, Practical Law Practice Note w-015-8833.
65 Id.
69 Recently, the Southern District of New York showed some leniency toward businesses that are already engaged in efforts to make their websites or mobile apps accessible. In Diaz v. The Kroger Company, the court held that held that an ADA web access claim is rendered moot where: (1) a defendant undertook compliance with the WCAG standards before the lawsuit was filed; (2) the website is presently compliant; (3) an affidavit confirmed that the specific barriers encountered by the plaintiff had been addressed; and (4) the defendant had no intention of undoing the changes and planned to keep their website compliant. Diaz v. Kroger Co., No. 18 CIV. 7953 (KPF), 2019 WL 2357531, at *3 (S.D.N.Y. June 4, 2019). See also Stephanie A. Sheridan & Michael A. Keogh, Hot Off the
B. **Requirements for ADA Compliance**

While the ADA regulations provide very detailed requirements for removal of barriers to disabled individuals in physical locations, no regulations have been enacted specifying what a business must do in order to make its virtual spaces accessible. In 2010, the DOJ issued an Advanced Notice of Proposed Rulemaking stating that it was considering establishing regulations to the ADA to address accessibility for individuals with disabilities on websites of public accommodations and requested public comment. ADA website accessibility regulations were expected to be issued in 2015. However, in 2017 the DOJ withdrew the Anticipated Notice of Proposed Rule Making, but reiterated that it had long considered websites to be public accommodations. The DOJ reaffirmed its position in a September 2018 letter to Congress by stating, “The Department first articulated its interpretation that the ADA applies to public accommodations’ websites over 20 years ago.”

In the absence of regulations, public accommodations using mobile apps to provide goods and services have been left with a number of questions as to what steps they need to take in order to ensure their mobile apps comply with the ADA. However, the DOJ has provided businesses with some guidance. In its settlement agreements with private business pertaining to the accessibility of websites, the DOJ has required that businesses bring their website into conformance with the World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (WCAG) version 2.0 Success Criteria Level AA. The DOJ’s view of conformance with WCAG 2.0 as a means to achieve ADA compliance has also been adopted by courts and private plaintiffs. For example, in June 2017, in the first-ever web accessibility decision after trial, the U.S. District Court for the Southern District of Florida found that Winn-Dixie supermarket’s website was a place of public accommodation because it was heavily integrated with the physical supermarket and the court ordered Winn-Dixie to bring its website into conformance with WCAG 2.0. While the DOJ and courts have generally accepted WCAG as the go to standard for web accessibility and mobile app accessibility, in its September 2018 letter to Congress, the DOJ stated its position that “noncompliance with a voluntary technical standard for website accessibility does not necessarily indicate noncompliance with the ADA.” In fact, the Ninth Circuit recently observed that the lack

---


70 75 Fed. Reg. 43460-01 (July 26, 2010).
74 The decision did not state whether conformance with Level A, Level AA, or Level AAA success criteria was required.
of specific instructions as to what businesses must do make their websites and mobile app accessible might be purposeful, in order to give businesses flexibility.\footnote{Robles v. Domino’s Pizza, LLC, 913 F.3d 898, 908 (9th Cir. 2019). Domino’s is seeking review of the Ninth Circuit’s decision by the U.S. Supreme Court. See https://linkprotect.cudasvc.com/url?a=https%3a%2f%2fwww.eater.com%2f2019%2f7%2f8%2f930669%2fdominos-supreme-court-website-accessibleblindusers&c=E,1,I12gHickvjQ6vynoM9S2u2ERTfIB7GV0mbj_lwcaVmS5Pl9wBuPaZm9Epge2FkKPdLhop8nsZ7n89HKCCLMHyBTgDCrogmZJlePz7xmujFaZs,&typo=1 (last visited Aug. 16, 2019).}

The WCAG is a voluntary standard promulgated by the W3C, which does not have the force of law.\footnote{Shawn Lawton Henry, Web Content Accessibility Guidelines (WCAG) Overview, W3C (June 22, 2018), http://www.w3.org/WAI/standards-guidelines/wcag/.} However, as the DOJ, courts, and private plaintiffs have noted, it provides useful guidance on how to remove barriers to accessibility on websites and mobile apps in an effort to comply with the ADA. It consists of twelve guidelines for presenting the user interface in a way that users with disabilities can perceive, operate, understand, and interpret using a wide variety of assistive agents, including screen readers.\footnote{Id.} In addition, W3C has published instructional materials on how to apply WCAG to mobile websites and applications.\footnote{Shawn Lawton Henry & Julie Brewer, Mobile Accessibility at W3C, W3C (March 1, 2019), http://www.w3.org/WAI/standards-guidelines/mobile/#intro.}

C. Allocating ADA Compliance Responsibilities Between Developer and Franchisor

In considering the allocation of ADA compliance responsibilities between the developer and the franchisor, franchisors should think about ADA compliance with respect to the developer’s deliverables, as well as ADA compliance for any third-party content linked to the mobile app. The allocation of responsibility for ADA compliance will often depend on the scope of work as well as the other obligations of the parties under the contract. If the franchisor is contracting with a developer to develop a mobile app with features that are an extension of its sale of goods and services, such as online ordering, the franchisor may want to specify in the development contract that the developer is responsible for delivering a mobile app that meets WCAG 2.0 AA or other agreed upon web accessibility criteria. In addition, franchisors may want the developer to indemnify the franchisor from any ADA claims arising out of or related to developer’s failure to meet their obligation to build the mobile app to a specified web accessibility guideline. With the absence of regulations specifying exactly what features a mobile app needs to have in order to be compliant with the ADA and other accessibility laws, franchisors may find that developers are unwilling to warrant that the mobile app complies with the ADA, but may be willing to warrant conformance with a particular accessibility standard, such as WCAG. In addition, franchisors should be mindful of any areas of ADA compliance that are not the developer’s responsibility. For example, an ADA claim pertaining to franchisor developed content or pertaining to the height of the shelf that a customer must reach in in a restaurant in order to pick up a mobile order.

Franchisors should also consider the allocation of responsibility for ADA compliance of third-party content, including developer content that is linked to the mobile app. If the mobile app links to a payment processing page that is managed by a developer, the franchisor should consider contract language requiring the vendor to comply with a particular accessibility standard, such as WCAG. For example, in \textit{Gil v. Winn Dixie Stores, Inc.}, the court found that there were...
six different third parties, including Google and American Express, who interface with Winn-Dixie’s website and that Winn-Dixie has an obligation to make sure that those third parties also ensure that their websites are accessible.\textsuperscript{80}

D. Vicarious Liability Issues

While it is often clear that the franchisee is subject to the requirements of Title III of the ADA, a franchisor’s liability under the ADA often depends on whether the franchisor exercises sufficient control over a specific aspect of the business, such that it is considered an operator. As the leading case on this area, \textit{Neff v. American Dairy Queen Corp.} notes, a franchisor is only an “operator” if it “specifically controls” its franchisee with respect to the “allegedly discriminatory conditions”.\textsuperscript{81} While franchisor liability under the ADA has traditionally been analyzed in the context of physical barriers to access, such as a lack of handicap accessible parking, or pertaining to an aspect of the operations in the place of business, such as refusal to admit a customer’s service animal, questions regarding the accessibility of websites and mobile apps provide a new context in which to analyze this issue. Franchisors that design and have developed mobile apps for use by their franchisees’ customers may find themselves subject to ADA lawsuits pertaining to the alleged inaccessibility of the mobile app to disabled customers. They may also see claims for indemnification or breach of contract, among other possible claims, brought against them by their franchisees.

VIII. OTHER ISSUES

There are a number of additional legal requirements that franchisors should consider when developing a mobile app and launching it for use by the franchise system. Laws pertaining to menu labeling and disclosure of ingredients and nutritional information, truth-in-advertising and marketing to children, and consent to send text messages (SMS) and email, are just a few of these.

A. Compliance with Menu Labeling Requirements by Food Service Providers

Franchisors in the food service industry should consider the applicability of menu labeling laws to content that is posted on the mobile app. This is especially true in instances where a restaurant’s menu will be posted on the mobile app and/or customers will be able to place food orders through the mobile app. As of May 7, 2018, the Food and Drug Administration (FDA) Menu Labeling Rule\textsuperscript{82} was issued to help implement the calorie and nutrition information requirements of the Food, Drug, and Cosmetic Act (FDCA).\textsuperscript{83} As a result of the passage of this legislation, certain restaurants and other food sellers must comply with the FDA regulations requiring specific calorie and nutrition information on menus.\textsuperscript{84} The Menu Labeling Rule requires that covered establishments post: calorie information or the number of calories in each listed standard menu item, food item on display, or self-service food item, as usually prepared or offered for sale; a succinct statement on suggested daily calorie intake similar to “2,000 calories a day is used for


\textsuperscript{81} Neff v. American Dairy Queen Corp., 58 F.3d 1063, 1066–67 (5th Cir. 1995).

\textsuperscript{82} 21 C.F.R. § 101.11 (2019).

\textsuperscript{83} FDCA §§ 403(q)(5), 403A (2019).

\textsuperscript{84} 21 C.F.R. § 101.11.
general nutrition advice as the suggested amount, but individual needs may vary; and the statement “Additional written nutrition information is available upon request”, and if this information must be provided if ever requested. The Menu Labeling Rule governs covered establishments, which are defined as establishments serving restaurant-type food that: are part of a chain of twenty or more locations, do business under the same name, and offer substantially the same menu items. Covered establishments include restaurants, convenience stores, grocery stores, takeout facilities and delivery facilities, entertainment venues, cafeterias, coffee shops, and supermarkets. Certain types of establishments are exempt from the rule, including establishments that provide free food served to employees or consumers, mobile vendors such as those in sports stadiums or on trains, in-patient only food service, and catering services to the extent that they are not part of a restaurant that is otherwise a covered establishment. The Menu Labeling Rule defines “restaurant-type food” as foods that are usually eaten on the premises, while walking away from the premises, or soon after arriving at another location.

If a business is covered, does it need to display calorie and nutrition information on its mobile app? Covered establishments are required to post calorie information about their standard menu items on their menus and menu boards, referred to in the Menu Labeling Rule as primary writings. Primary writings can include menus on the Internet, and in determining whether a menu is a primary writing a business should look at factors such as whether the writing lists the name or picture of the standard menu item and the associated price and whether the writing can be used by the customer to make an order selection while the customer is viewing the writing. Marketing materials such as coupons, signs, posters, or paper inserts are not considered menus. If the writing meets these requirements, the business must post calorie information for each standard menu items next to the respective food item in a manner that is: clear and prominent; no smaller than the size of the name or the price of the standard menu item it refers to, whichever is smaller; and in the same color or a similar color as the color used for the name of the standard menu item. If there are multiple options on the menu for ways in which a standard menu item may be prepared, the covered establishment must list the calories separately for each flavor, size, or extra toppings listed on the menu.

If calorie or related nutrition information is absent or inaccurate, the foods may be deemed misbranded and subject to the penalties for misbranding under the FDCA. The FDA does not have any new or additional enforcement mechanisms specific to menu labeling. Accordingly

85 Id.
86 Id.
88 21 C.F.R. § 101.11
89 Id.
90 Id.
91 Id.
92 Id.
93 21 C.F.R. § 101.11
94 Id.
violators may be imprisoned for up to one year, fined up to $1,000, or both. For a subsequent conviction of misbranding, or commission of the felony of misbranding with the intent to defraud or mislead, the violator is subject to up to three years imprisonment, fined up to $10,000, or both. In addition, the FDA may bring a civil action in federal court to enjoin a violator and any misbranded food is subject to seizure. The FDA has stated that it will work cooperatively with covered establishments during the first year of implementation and intends to allow for reasonable opportunities to correct minor violations.

While a number of states had enacted menu labeling laws prior to the federal rules taking effect, on its face the menu labeling provisions of the FDCA contain an express federal preemption clause at 21 U.S.C. § 343-1, which states that “no State or political subdivision of a State may directly or indirectly establish ... any requirement for nutrition labeling of food that is not identical to the requirement of section 343 (q) of this title [which contains restaurant menu labeling requirements].” For example, the New York City Health Code requires New York City food service establishments that are part of a chain operating fifteen or more locations and offer substantially the same menu items at each location to post a salt shaker icon next to any food item or combination meal containing 2300 mg or more of salt, and the following language explaining the icon's meaning: “the sodium (salt) content of this item is higher than the total daily recommended limit (2300 mg).” Businesses with mobile apps that will be used by consumers in California should also consider the application of California’s Proposition 65 chemical warnings legislation. Given that the California law requires that the consumer be warned about the presence of certain chemicals prior to exposure, a business may be required to post the required warning on its mobile app, particularly where there may be remote ordering through the mobile app.

During mobile app development, businesses will want to consider the extent to which federal and state menu labeling laws apply to the content on the mobile app and who is responsible for ensuring compliance. For instance, is the responsibility on the developer, the franchisor's marketing team, or possibly the franchisee if the franchisee will be adding menu content? Businesses may also want to consider how the menu information on the mobile app will change based on the geographic location of the user.

B. Providing Technology to Permit Customers To Identify Food Allergy Issues

Food business franchisors might also consider whether content can be posted on the mobile app that can assist the franchisor or franchisees in providing customers with easier access to information regarding food allergens, as well as compliance with state laws. Providing customers with access to information regarding allergens in food not only promotes good

95 21 USCA § 333 (2019).
96 Id.
97 Id.
100 CAL. HEALTH & SAFETY CODE § 25249.6 (2019).
101 Id.
customer service, but it may also help to prevent a serious health and safety risk and in some instances may be a legal requirement. Depending upon the severity of the allergic response, a food allergy may be a disability within the scope of the ADA.\textsuperscript{102} In such instances, the business, if a public accommodation, may be required under the ADA to take reasonable steps to accommodate individuals with disabilities where it does not result in a fundamental alteration of that restaurant’s operations. Such reasonable steps may include answering questions about ingredients in a menu item.\textsuperscript{103} While businesses may still have an obligation to ensure that staff is adequately trained to answer questions about allergens, the mobile app can be a useful tool to assist in getting accurate ingredient information to customers. In addition to obligations under the ADA, Illinois,\textsuperscript{104} Maryland,\textsuperscript{105} Massachusetts,\textsuperscript{106} Michigan,\textsuperscript{107} Rhode Island,\textsuperscript{108} Virginia,\textsuperscript{109} New York City,\textsuperscript{110} and Saint Paul, Minnesota\textsuperscript{111} have enacted laws specifically addressing access to information about allergens and/or employee training on allergens in restaurants. Among other requirements, the allergen awareness laws in Massachusetts\textsuperscript{112} and Rhode Island\textsuperscript{113} require food service establishments to post a notice on printed menus and menu boards, requesting that customers notify their server if a person in their party has a food allergy. For businesses selling pre-package foods, the Food Allergen Labeling Consumer Protection Act (FALCPA), contains allergen labeling requirements applicable to packaged FDA regulated foods.\textsuperscript{114} Business selling products that are subject to FALCPA must label packaged foods containing milk, eggs, fish (e.g., bass, flounder, cod), Crustacean shellfish (e.g., crab, lobster, shrimp), tree nuts (e.g., almonds, walnuts, pecans), peanuts, wheat, and soybeans as containing a “major food allergen.”\textsuperscript{115}

As it relates to mobile apps, businesses developing a mobile app that contains information about food products sold by the business should consider how they might inform customers using the mobile app of allergens contained in certain food items. Another consideration is how franchisees and their employees will be trained and prepared to respond to customer inquiries and requests related to allergens. For instance, if a customer will be placing a food order through

---

\textsuperscript{102} Questions and Answers About the Lesley University Agreement and Potential Implications for Individuals with Food Allergies, U.S. DEP’T OF JUST. (Jan. 25, 2013), https://www.ada.gov/q&a_lesley_university.htm.

\textsuperscript{103} Id.

\textsuperscript{104} 410 ILL. COMP. STAT. ANN. 625/3.07 (2019).

\textsuperscript{105} MD. CODE ANN., HEALTH-GEN. § 21-330.2 (West) (2019).

\textsuperscript{106} 105 MASS. CODE REGS. § 590.011 (2019).

\textsuperscript{107} MICH. COMP. LAWS ANN. § 289.6152 (2019).


\textsuperscript{110} NEW YORK CITY ADMINISTRATIVE CODE § 17-195 (2019).

\textsuperscript{111} SAINT PAUL LEG. CODE § 331A.11 (2019).

\textsuperscript{112} 105 MASS. CODE REGS. § 590.011 (2019).


\textsuperscript{115} Id.
the mobile app, will the mobile app provide a means for customers to inform the franchise location fulfilling the order of customer allergies?

C. Issues for Sites Marketing to Children

Depending on the content of the mobile app, franchisors may also need to consider the application of laws placing restrictions on marketing to children. The Children’s Online Privacy Protection Act (COPPA)\(^\text{116}\) applies to operators of websites and online services that are directed to or knowingly collect information online from children under age thirteen. The term “online services” is broad and includes mobile apps.\(^\text{117}\) Entities covered under COPPA must obtain verifiable parental consent before collecting, using, or disclosing personal information obtained from children.\(^\text{118}\) COPPA also requires the display of or link to a notice informing parents about the site’s collection, use, and disclosure practices.\(^\text{119}\) Parents must also be given the option to block future collection and to review information already provided by their children.\(^\text{120}\) This means that if a parent asks, you must: give them a way to review the personal information collected from their child; give them a way to revoke their consent and refuse the further use or collection of personal information from their child; and delete their child’s personal information.\(^\text{121}\) Covered website and mobile app operators are also required to adopt reasonable procedures for data retention and deletion. In 2017, the FTC released a step-by-step plan for companies to determine if they are covered by COPPA and how to comply.\(^\text{122}\) COPPA violations may be treated as unfair or deceptive acts or practices under Section 18(a)(1)(B) of the Federal Trade Commission Act and subject to FTC enforcement actions.\(^\text{123}\) Penalties for violations may include injunctive relief, civil penalties, and consumer redress.\(^\text{124}\) A court can hold operators who violate COPPA liable for civil penalties of up to $42,530 per violation.\(^\text{125}\) The amount of civil penalties a court assesses may turn on a number of factors, including the egregiousness of the violations, whether the operator has previously violated COPPA, the number of children involved, the amount and type


\(^{117}\) Id.

\(^{118}\) “Acceptable methods for obtaining a parent’s verifiable consent include having the parent: sign a consent form and send it back to you via fax, mail, or electronic scan; use a credit card, debit card, or other online payment system that provides notification of each separate transaction to the account holder; call a toll-free number staffed by trained personnel; connect to trained personnel via a video conference; provide a copy of a form of government issued ID that you check against a database, as long as you delete the identification from your records when you finish the verification process; answer a series of knowledge-based challenge questions that would be difficult for someone other than the parent to answer; or verify a picture of a driver’s license of other photo ID submitted by the parent and then comparing that photo to a second photo submitted by the parent, using facial recognition technology.” Children’s Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business, FED. TRADE COMMISSION (June 2017), https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance.

\(^{119}\) Id.

\(^{120}\) Id.

\(^{121}\) Id.

\(^{122}\) Id.


\(^{124}\) Id.

\(^{125}\) Id.
of personal information collected, how the information was used, whether it was shared with third parties, and the size of the company.\textsuperscript{126}

The FTC has brought many enforcement actions for violations of COPPA, most of which have resulted in settlements and consent decrees. The FTC’s largest COPPA related civil penalty to date was $5.7 million, which the music social networking site Musical.ly agreed to pay in February 2019 in order to settle allegations that the company knew many children were using the app but they still failed to seek parental consent before collecting names, email addresses, and other personal information from users under the age of thirteen.\textsuperscript{127} In addition to payment of the penalty, the company agreed to comply with COPPA requirements going forward.\textsuperscript{128} Franchisors should also consider whether they are subject to COPPA requirements even though they may not think that their mobile app is specifically marketed toward children. In 2014 Yelp, Inc. agreed to settle FTC charges that it improperly collected children’s information in violation of COPPA by failing to follow the COPPA rule’s requirements even though the company knew, based on the registrant’s birth dates, that children were signing up for Yelp through its mobile app.\textsuperscript{129} The company was also charged with failing to implement a functional age-screen in its apps and to adequately test its apps to ensure that users under the age of thirteen were prohibited from registering.\textsuperscript{130} The FTC’s complaint alleged that Yelp violated the COPPA rule by failing to provide notice to parents of its information practices, and to obtain verifiable parental consent prior to collecting, using, or disclosing personal information from children under thirteen when it knew that it was collecting personal information from children under thirteen via the Yelp App.\textsuperscript{131}

In addition to the requirements of COPPA, this area is also self-regulated by the Council of Better Business Bureaus. The Children’s Advertising Review Unit (CARU) of the Council of Better Business Bureaus evaluates child-directed advertising and promotional material in all media to advance truthfulness, accuracy and consistency with CARU’s Self-Regulatory Program for Children’s Advertising, including CARU’s guidelines (Guidelines), and relevant laws.\textsuperscript{132} CARU monitors advertisements found in broadcast and cable TV, radio, children’s magazines, comic books, the Internet and mobile services for compliance with its Guidelines. In addition, CARU handles consumer complaints. When ads are found to be misleading, inaccurate, or inconsistent

\begin{footnotes}
\item[130] Even though Yelp’s privacy policy states that Yelp is not directed to children under 13, because Yelp collected personal information from consumers who input birthdates during the user registration process indicating that they were under 13, the FTC deemed Yelp to have had “actual knowledge” under the COPPA Rule that it was collecting personal information from children under 13. Cynthia J. Larose & Julia M. Siripurapu, Time to Step Up Your COPPA Compliance, MINTZ LEVIN (Sept. 25, 2014), https://www.mintz.com/newsletter/2014/Advisories/4292-0914-NAT-PRIV/index.html.
\item[131] Id.
\end{footnotes}
with its Guidelines, CARU seeks changes through voluntary cooperation. The results of CARU inquiries are publicly recorded in the National Advertising Division/CARU Case Reports. Businesses are generally advised to take CARU inquiries seriously, as CARU regularly refers companies that do not cooperate to the FTC and the FTC treats CARU referred cases with priority.

Similar to COPPA, CARU has issued Guidelines addressing the online collection and use of data submitted by children under age thirteen. The CARU Guidelines provide that tracking practices and the collection and use of information must be clearly disclosed along with the means of correcting or removing information. In addition, they require that prior verifiable parental consent be obtained when personal information will be publicly posted or distributed to third parties. Pursuant to the CARU Guidelines, a parent must be directly notified of the nature and intended uses of information collected and retained to respond more than once to a child’s specific request and parents must be given sufficient access to allow for the removal and correction of the information.

Businesses should carefully consider what information, if any, the mobile app is collecting from children under thirteen. Even if the mobile app is not targeted to children, businesses could still face regulatory action if they have sufficient information about mobile app users to know that there are users under the age of thirteen. As a result, at least a general awareness of COPPA requirements and CARU Guidelines may be beneficial to all businesses developing mobile apps, regardless of whether the business intends the mobile app to be used by children. Businesses developing mobile apps might also consider participation in CARU’s COPPA safe harbor program, which was established by CARU to provide guidance to companies on how to comply with COPPA and CARU Guidelines. Program participants who adhere to CARU’s Guidelines are deemed in compliance with COPPA and essentially insulated from enforcement actions by the Federal Trade Commission (FTC).

**D. Application of TCPA, CSPAM, and Related Statutes**

Businesses often plan to send out messages in conjunction with a mobile app program, either through SMS, email, or push notification. For example, if a customer places a remote order through a mobile app, the business may want to send the customer an SMS notification when the order is ready. The business may also want to send an email or SMS to customers offering a discount on orders placed through the mobile app or an update on loyalty points. While the ability to utilize these channels to communicate may be convenient and may even help drive traffic to the mobile app or the franchise business, the use of phone calls, SMS, or email to communicate comes with some legal risk. Due in part to increased prevalence of SMS marketing, confusion

---

133 Id.

134 Id.


136 Id.


regarding the requirements for TCPA compliance, the TCPA’s statutory damages, and the relative ease with which the law lends itself to class action claims, the number of TCPA lawsuits filed has increased significantly in recent years.

Businesses utilizing SMS or calling as a means to communicate, whether it be with customers, franchisees, or others, should be aware of the requirements of the Telephone Consumer Protection Act (TCPA). Enacted in 1991 to address consumer frustrations with robocalls and junk faxes, the TCPA covers calls made to residential and wireless phone lines as well as fax transmissions.\textsuperscript{139} The TCPA places restrictions on calls made to consumers in violation of Do-Not-Call Requests, telemarketing calls to residential lines, telemarketing and informational calls and SMS to wireless lines, and other prohibited calls pertaining to medical facilities and emergencies.\textsuperscript{140} The TCPA’s prohibitions on calls, including SMS, are affected by whether the equipment used to make the call qualifies as an automated telephone dialing system (ATDS), on whether the correct form of consent is obtained, and on whether the content of the call or SMS is telemarketing or informational.\textsuperscript{141} It provides for a private right of action and the potential for recovery of statutory damages of $500 to $1,500 per violation (i.e. per call, text or fax sent), among other relief.\textsuperscript{142}

As it relates to mobile apps, the majority of the legal activity with respect to the TCPA is in the area of wireless calls and SMS made using an ATDS. The TCPA defines an ATDS as, “equipment which has the capacity – (A) to store or produce telephone numbers to be called, using a random or sequential number generator; and (B) to dial such numbers.”\textsuperscript{143} The TCPA, as interpreted through the FCC’s regulations and declaratory rulings, prohibits making any call using an ATDS or an artificial or prerecorded voice to a cellphone number without prior express consent, unless the call is for an emergency purpose.\textsuperscript{144} If the call made to a cellphone number using ATDS or an artificial or prerecorded voice “includes or introduces an advertisement or constitutes telemarketing”, the prior express consent must be in writing.\textsuperscript{145} In providing prior express written consent, the individual must clearly authorize the company to deliver telemarketing messages to the consumer using automated means, specifically name the company to whom the consent is provided, specify the consumer’s phone number, disclose that the consumer is not required to provide consent as a condition of purchasing products or services, and obtain the consumer’s signature either electronically or handwritten.\textsuperscript{146} The FCC has stated in its declaratory rulings that an individual can use “any reasonable means” to revoke consent.\textsuperscript{147}

While the FCC had taken an expansive view as to what qualifies as an ATDS, stating that “capacity” includes “its potential functionalities” or “future possibilities” of the calling equipment, last year the DC Circuit struck down the FCC’s interpretation of ATDS in its much anticipated

\begin{footnotes}
\item[140] \textit{Id.}
\item[141] \textit{Id.}
\item[142] § 227 (c)(5).
\item[143] § 227(a)(1).
\item[145] \textit{Id.}
\item[146] \textit{Id.}
\item[147] \textit{Id.}
\end{footnotes}
decision in *ACA International v. FCC*.\(^{148}\) In addition, the DC Circuit struck down the FCC’s one call safe harbor for calls made to reassigned numbers as arbitrary and capricious.\(^{149}\) Therefore, in the wake of the DC Circuit’s decision in *ACA International*, we are left with the text of the TCPA and courts’ interpretations of the statute and whether ACA International also struck down the FCC’s interpretation of ATDS and treatment of reassigned phone numbers as stated in its rulings prior to the 2015 Ruling that was the subject of ACA International. The Second, Third, and Ninth Circuit have all rendered noteworthy decisions on the issue of what constitutes an ATDS in light of *ACA International*. While the Second Circuit\(^{150}\) and Third Circuit\(^{151}\) have both interpreted the TCPA definition of ATDS to mean the equipment must have the present capacity to generate random or sequential numbers, the Ninth Circuit has come out differently on this issue. In *Marks v. Crunch San Diego*, LLC the Ninth Circuit adopted a broader definition of ATDS, finding that technology qualifies as an ATDS if it 1) has the present ability either to a) store telephone numbers to be called; or b) produce telephone numbers to be called using a random or sequential number generator and 2) can dial such numbers.\(^{152}\) Under the more expansive Ninth Circuit view, the technology need not have a random or sequential number generator.\(^{153}\) In *Marks*, the Ninth Circuit also held that *ACA International* invalidated not only the July 2015 FCC Order, but also the FCC’s prior rulings determining whether technology qualifies as an ATDS.\(^{154}\) However, other courts have taken the view that *ACA International* did not invalidate any FCC rulings on the definition of ATDS prior to the FCC’s 2015 TCPA Ruling, as the timeframe to challenge those rulings had passed.\(^{155}\) Uncertainty in the courts’ interpretation of the TCPA is likely to continue until the FCC or Congress takes further action. On May 14, 2018, the FCC issued a public notice requesting comment on the definition of an ATDS, the treatment of calls made to reassigned wireless numbers and the meaning of “called party”, and the methods for revocation of consent, but it has not taken further action toward issuing and updated ruling since.

Businesses that plan to contact mobile app users by phone call or text message in connection with their mobile app program should have TCPA compliance in mind. In light of the jurisdictional splits following *ACA International* and until the FCC provides further clarification, businesses continue to face uncertainty as to whether the equipment they are using to make calls or send SMS to customers is exempt from the coverage of the TCPA. Consequently, businesses that plan to send SMS or make phone calls to mobile app users should consider how consent will be obtained from the customer in light of TCPA requirements. While the prior express consent to make informational calls or SMS to the customer, such as a notification that the customer’s order is ready, need not be in writing,\(^{156}\) businesses should keep in mind that as a practical matter, the burden will be on the business as the caller, to show that it has obtained prior express consent. Furthermore, depending on the specific content of the call or SMS, the business may face disputes as to whether the content is informational or advertising in nature. In light of these

---

\(^{148}\) *ACA International v. FCC*, 885 F.3d 687 (D.C. Cir. 2018).

\(^{149}\) *Id.*

\(^{150}\) King v. Time Warner Cable Inc., 894 F.3d 473 (2d Cir. 2018).

\(^{151}\) Dominguez *ex rel.* Himself v. Yahoo, Inc., 894 F.3d 116 (3d Cir. 2018).

\(^{152}\) Marks v. Crunch San Diego, LLC, 904 F.3d 1041 (9th Cir. 2018), *cert. dismissed*, 139 S. Ct. 1289, 203 L. Ed. 2d 300 (2019).

\(^{153}\) *Id.*

\(^{154}\) *Id.*


\(^{156}\) 30 FCC Rcd. at 7967
concerns, businesses might consider whether it is appropriate to obtain prior express written consent from mobile app users before sending calling or sending them SMS, regardless of whether the content of the call or SMS is informational of advertising. As noted above, if the business intends to make marketing calls or sending marketing SMS to users of the mobile app, it will need to obtain prior express written consent. Businesses should consider how they will obtain the customer’s written consent. Will it be through the mobile app itself? How will the business keep records of the customer’s consent? Will the customer have the ability to revoke consent through the mobile app or by other “reasonable means”? How will the business keep track of revocations of consent? Furthermore, how will the business check to ensure that the phone number has not been reassigned to an individual who has not given consent? It is also worth noting that the TCPA requirements pertain to attempts to communicate with consumers by telephone. Mobile app programs often communicate with users through push notifications, which may not be subject to TCPA requirements if sent over the Internet.

Another means that businesses may choose to use to communicate with their customers about their mobile app program is through email. For instance, if a business has a large number of email subscribers, it may want to send out an email blast to its subscriber list to let them know about the mobile app or offers that encourage subscribers to download the mobile app. Businesses employing these techniques should be aware of laws pertaining to email marketing, primarily the CAN-SPAM Act. In 2003 Congress enacted the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act)157 to regulate unsolicited commercial emails. The CAN-SPAM Act does not flatly prohibit unsolicited commercial emails, but it does set out specific requirements for the content of these messages and contain requirements to ensure that consumers can opt-out of receiving them. The CAN-SPAM Act regulates the transmission of all commercial emails, not just unsolicited emails.158 A commercial email is defined in the Act as an email message that has a “primary purpose of...commercial advertisement or promotion of a commercial product or service.”159 Emails sent to consumers that have a primary purpose pertaining to a particular transaction or relationship between the sender and the consumer are exempted from the CAN-SPAM Act’s requirements for commercial messages.160 Even if the email contains some commercial content, the primary purpose of the email needs to be commercial in order to trigger coverage. The law places responsibility for compliance with CAN-SPAM Act requirements on the initiator of the commercial email message, meaning the one who originates or transmits the message or that procures the transmission of the message.161

The CAN-SPAM Act prohibits the initiation of a transmission of a commercial or transaction message or relationship message that contains false or misleading transmission information as to the initiator of the message.162 The CAN-SPAM Act also prohibits deceptive subject headings in commercial emails.163 Furthermore, the CAN-SPAM Act requires initiators of a commercial email to include in the commercial email: clear notice of the recipient’s right to opt-out of future messages from the sender of the email and one of the following opt out mechanisms

159 Id.
160 § 7702(2)(B).
162 § 7704(a)(1).
163 § 7704(a)(2).
a) a functional return email address, allowing the recipient to simply “reply” to the email indicating the recipient’s opt out; or b) another internet based opt-out mechanism. The opt-out mechanism must be functional for thirty days after the message is sent.

The FTC is the primary enforcer of the CAN-SPAM Act, but various federal, state, and private parties may also bring claims for violations. The FTC has authority to enforce the CAN-SPAM Act as if a violation were an unfair or deceptive act or practice prohibited under the FTCA and can seek civil penalties of up to $16,000 for each separate violation (if based on knowledge or knowledge fairly implied) and injunctive relief (does not require a showing of knowledge). Other agencies including but not limited to the FCC, the Federal Reserve Board, the SEC, and the Secretary of Transportation may enforce the CAN-SPAM Act where it relates to activities outside of the FTC’s jurisdiction and Internet Service Providers may bring actions under the CAN-SPAM Act in certain instances. The penalties for non-compliance in such actions will depend on the regulatory regime enforced by the agency bringing the action. The CAN-SPAM Act also authorizes states attorneys general, officials, and other agencies to bring claims for CAN-SPAM Act violations against residents of the state and seek injunctive relief, damages for actual loss or statutory damages of up to $250 per violation, whichever is greater, with a maximum award of $2,000, the costs of bringing the action and reasonable attorney’s fees. With respect to the damages caps, claims for false or misleading headers are not subject to the cap. In addition the state may recover three times the amount of statutory damages for willful, knowing or aggravated violations.

IX. CONCLUSION

Mobile apps, online ordering programs, and loyalty programs bring with them significant opportunities for franchise systems. These opportunities include greater engagement with customers—including young customers—and greater ability to retain customers and earn repeat business.

With these opportunities come risks. A franchise system developing a mobile app needs to be aware of compliance with various statutory and regulatory schemes, including the ADA and those statutory and regulatory schemes related to data privacy, electronic fund transfers, and food labeling. Further, there are a host of practical considerations for a franchise system developing a mobile app: negotiating with app developers, communicating the benefits of the app to franchisees, executing the rollout of the app, arranging insurance coverage for the risks associated with the app, as well as ensuring franchisee compliance with app implementation and app-based customer loyalty programs.

Nevertheless, given the opportunities for profit and growth associated with developing and deploying a mobile app, franchise systems should consider whether developing an app is right for them. Each franchise system considering development and deployment of a mobile app needs to take an individualized approach to weighing the potential benefits against the potential risks. And because the laws, technology, and practical considerations around mobile app development

164 § 7704(a)(5).
165 Id.
168 § 7706(f)(3)(C).
continue to evolve, each franchise system needs to continue to monitor this evolution and be ready to modify their utilization of mobile apps.
Gary R. Batenhorst

Gary R. Batenhorst is a partner in the Omaha, Nebraska office of Cline Williams Wright Johnson & Oldfather, L.L.P. He concentrates his practice on franchise transactional and compliance matters, representing primarily franchisors, product manufacturers, and multi-unit franchisees. He also represents start-up franchisors in the establishment and development of franchise systems. Gary was in-house counsel for Godfather’s Pizza, Inc. from 1983-2001. He taught Franchising as an Adjunct Professor at Creighton University School of Law for fourteen years, where he currently teaches Business Planning. Gary received his B.S.B.A. from Creighton University and his J.D. from New York University School of Law. Gary served as Editor-in-Chief of the Franchise Law Journal from 2015 to 2018, currently serves on the Governing Committee of the Forum on Franchising, and is the Forum’s Publications Officer.

Lindsey Cooper

Lindsey Cooper is Managing Corporate Counsel in the Dispute Resolution Group at Franchise World Headquarters, LLC, which provides legal counsel to the Subway® franchisor and related business entities and management of litigation/arbitration matters involving the Subway® System. Prior to joining the Subway® Legal Department, she was a law clerk at Edible Arrangements International. Lindsey received her B.S. in Business Management from Providence College and her J.D. from Quinnipiac University.

Daniel Graham

Daniel Graham is an Associate in Perkins Coie LLP’s Denver office. He has experience working on all phases of complex litigation, including franchise litigation. He is the past chair of the Colorado Bar Association Franchise Subsection, as well as a past Executive Council Member for the Business Law Section of the Colorado Bar Association. Currently, he is on the Board of the Faculty of Federal Advocates. In 2019, Dan was named as a Super Lawyers Rising Star for Civil Litigation. Dan received his B.A. from the University of Montana and his J.D. from the University of Denver, graduating first in his class.