The Soul of Franchising

October 14-16, 2015
Sheraton New Orleans Hotel New Orleans, LA
W-17 Life in the Fast Lane: Electronic/Mobile Pay Programs and Data Privacy Standards

Carol Anne Been, Dentons US LLP
Brian Carroll, LevelUp
Keri McWilliams, Nixon Peabody LLP
What is a mobile payment?
Why should my client/business care about mobile payments?

• Staying State of the Art
• Customer Engagement
  – Targeted Customer Messaging
  – Reach New Customers
• Customer Convenience
• Cost Savings
• Ticket/Check Increases
What are the... advantages? risks?

- Security
- Consumer Data Collection
- Loyalty/Rewards Programs Adoption

- Security
- Consumer Data Collection
- Implementation Costs
What are the options?

- Mobile-Based Card Acceptance Devices
- Mobile Banking and Bill Pay
- Mobile Peer-to-Peer Payments
- Internet Commerce from a Mobile Device (and Online Ordering)
- Retail Point-of-Sale Mobile-Initiated Payments
- Mobile Gift Card Redemption
Frequently Asked Questions

• What is NFC?
• I don't have to learn about Bitcoin, right?
• What's best for the size of my franchise organization?
• What's best for our geography?
• What's best for our demographics?
Mobile Pay In Franchise Systems

• Should the franchisor address mobile payment systems, or can/should it let the franchisees do it on their own?
• Can the franchisor compel its franchisees to all use the same mobile payment system?
• Can franchisees opt-out?
The Franchise Agreement

• What sections of the franchise agreement should the franchisor review?
• Does the franchisor need to amend its franchise agreement?
• If the franchisor were drafting a new agreement, what should it include?
What is this going to cost? Who pays?

- Can the franchisor pay for the system out of its ad budget?
  - Development Fees?
  - Transaction Fees?
  - Monthly Fees?
- What should franchisees pay?
- Are there any hidden fees?
How will the mobile system integrate with existing POS, accounting and CRM systems?

- Will I need additional hardware?
- Will the franchisor's existing payment processor or POS provider object?
- How does this relate to the new EMV (chip and pin) standard?
Combining mobile-pay with loyalty or gift cards

- Who should control the design of a loyalty/rewards program?
- Who is responsible for the rewards earned and redeemed?
- Who is responsible for prepaid funds?
- Who benefits from breakage?
What does a mobile payment provider contract look like?

• Depends on what type of mobile system will be adopted
• Protections that a franchisor needs or should demand
• Also consider: Franchisee agreements
  User agreements
Key Contract Terms

• Development, hosting, maintenance, support
• Data collection and security
• Data analytics
• Loyalty and other marketing integration
• Intellectual Property, Data Ownership
• PCI Compliance
• Warranties, Indemnification
State and Federal Laws and Regulations to Consider (That You May Not Have Thought of Before)

- Data collection, security and privacy, e.g.:
  - GLBA, FTC Red Flags Rule, state laws on Data Breaches
  - PCI-DSS Standards
State and Federal Laws and Regulations to Consider (That You May Not Have Thought of Before)

• Consumer messaging and disclosures, e.g.:
  – Regulation E (CFPB); Section 5 of the FTC Act, UDAAP, CAN SPAM, TCPA, COPPA, Menu Disclosures Regs (FDA), and similar state laws
State and Federal Laws and Regulations Applicable to Providers

• Money laundering and payment fraud: e.g., FinCEN Regulations, CFPB
• State licensing of money transmitters (money services business)
• Gift card laws: Credit CARD Act, state laws governing disclosures and breakage
What's next?

• Online ordering/payment to replace the POS sales clerk and terminal

• How long before debit cards/credit cards go away?
LIFE IN THE FAST LANE:
ELECTRONIC MOBILE/PAY PROGRAMS
AND DATA PRIVACY STANDARDS

Carol Anne Been
Dentons
Chicago, Illinois

and

Brian Carroll
Levelup
Boston, Massachusetts

and

Keri McWilliams
Nixon Peabody
Washington, DC

October 14 – 16, 2015
New Orleans, LA

©2015 American Bar Association
# TABLE OF CONTENTS

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

II. BACKGROUND ................................................................................................................... 2  
   A. Key Terminology ............................................................................................................. 2  
   B. Existing Payment Methods .......................................................................................... 3  
      1. Cash (and electronic Stored Value) ........................................................................... 3  
         a. Stored Value (“Closed Loop”) ............................................................................. 3  
         b. Prepaid “Open-Loop” Cards .............................................................................. 3  
      2. Direct Pay from Bank (Checks and eChecks) ......................................................... 4  
      3. Debit and Credit Card Payments ............................................................................. 4  
         a. Traditional Card Payments ............................................................................... 4  
         b. Interchange Fees ............................................................................................... 4  
         c. EVM and Chip-and-Pin ...................................................................................... 5  
   C. Alternative Payment Methods .................................................................................... 5  
      1. Carrier Billing .......................................................................................................... 5  
      2. Cryptocurrency ....................................................................................................... 5  
   D. Mobile Payments ......................................................................................................... 6  
      1. Mobile Card Acceptance Devices .......................................................................... 6  
      2. Mobile Banking and Bill Pay .................................................................................. 7  
      3. Mobile Peer-to-Peer Payments ............................................................................... 7  
      4. Internet Commerce from a Mobile Device (and Online Ordering) ................. 7  
      5. Digital Content Purchases ...................................................................................... 7  
      6. Mobile Wallet ........................................................................................................ 8  
      7. Retail Point-of-Sale Mobile-Initiated Payments ................................................. 8  
      8. Mobile Gift Card Redemption ............................................................................... 9
E. The Positives and Negatives of Retail Mobile Payments

1. Customer Convenience .......................................................................................9
2. Security..............................................................................................................10
3. Branding ..........................................................................................................10
4. Consumer Data Collection .............................................................................11
5. Loyalty/Rewards Programs Adoption ..............................................................11
6. Cost Savings/Check Increases ..........................................................................11
7. Targeted Messaging to Existing Customers .....................................................12
8. Ability to Reach New Customers ......................................................................12
9. Implementation Costs ......................................................................................12

III. NEGOTIATION OF AGREEMENTS FOR RETAIL MOBILE PAYMENTS ..........13

A. Deal Structure ..................................................................................................13
B. Territory ............................................................................................................14
C. Development Agreement ..................................................................................14
D. Hosting ..............................................................................................................14
E. Training .............................................................................................................14
F. Maintenance and Support Services ....................................................................15
G. Customer Service ............................................................................................15
H. Bank/Credit Card Company Support ...............................................................15
I. Loyalty Programs ...............................................................................................15
J. Other Marketing Opportunities ..........................................................................16
K. Data Reporting and Analytics ..........................................................................16
L. Fees ..................................................................................................................17
M. Intellectual Property Ownership, Protection and Licensing .........................18
   1. Patents ............................................................................................................18
   2. Copyrights .....................................................................................................18
3. Trademarks ..............................................................................................19
4. Trade secrets and confidentiality............................................................20

N. Bankruptcy and Source Code Escrow ....................................................20
O. Data Ownership.....................................................................................21
P. Data Handling, Storage, Security, Retention and Destruction..............21
Q. Open Source ..........................................................................................22
R. Warranties..............................................................................................22
S. Indemnification .......................................................................................23
T. User Agreements ...................................................................................24

1. Privacy Policy .......................................................................................24
2. Terms of Service / Terms of Use............................................................25

U. Americans with Disabilities Act..............................................................25
V. Compliance with Laws and Regulations ..............................................26

1. Financial. ...............................................................................................26
   a. Banking regulators (Federal Reserve, FDIC, OCC, NCUA).................26
   b. State Licensing of Money Transmitters..........................................27
   c. Gift Card laws....................................................................................27
   d. Consumer Financial Protection Bureau (CFPB) .........................28
   e. Financial Crimes Enforcement Network (FinCEN)...............28
   f. Gramm-Leach-Bliley Act (GLBA) – Safeguards Rule and Data Privacy Rule; and State law equivalents ......29
   g. FTC Red Flags Rule...........................................................................29
   h. EMV Chip Cards - changes concerning fraud.................................29

2. Consumer Protection ..........................................................................30
   a. FTC Section 5....................................................................................30
   b. UDAAP (Unfair, Deceptive or Abusive Acts and Practices)...........31
   c. CAN SPAM .....................................................................................31
d. TCPA .................................................................32

3. Industry Standards / State Statutes.................................33
   a. PCI-DSS ..........................................................33
   b. State laws on data breach notification and data security .34
   c. State laws on consumer protection and marketing .......35

IV. FRANCHISING ISSUES IN MOBILE PAYMENT ..................36
   A. Key Drivers in Franchising................................................36
      1. Access to Customer Data ..............................................36
      2. Access to Revenue Stream ..............................................36
   B. Key Challenges in Franchising .............................................37
      1. Vicarious Liability .......................................................37
      2. Pricing ......................................................................37
      3. Adoption Issues .........................................................37
         a. Franchise Agreements ...............................................37
         b. Cost ....................................................................38
         c. Perceived Benefits ..................................................39

V. BEST PRACTICES.................................................................40
   A. Define Goals and Scope..................................................40
   B. Solicit Franchisee Feedback and Involvement ..................40
   C. Select Best Mobile Payment Platform for the System ........40
   D. Identify Needed Vendor(s) ...............................................40
   E. Negotiate Necessary Agreements with Vendors and Franchisees ....41
   F. Assess Compliance/Legal Issues ......................................41
   G. Develop Pilot Program ..................................................41
H. Rollout System-wide........................................................................................................42

V. CONCLUSION................................................................................................................................42
I. INTRODUCTION

In the early 1950’s, the restaurant industry revolutionized the way that customers paid for meals by accepting the very first credit card, offered by Diner’s Club. That innovation led quickly to the magnetic stripe credit card, which changed the way that consumers pay for everything at the retail point of sale. Sixty-five years later, credit and debit card payments, using the same plastic, magnetic stripe card, are entrenched as a social norm for retail point-of-sale (and now online retail) purchases. And the system still works exceptionally well. The magnetic stripe credit card persists after six-plus decades, because it is one of the most simple and efficient ways to conduct retail transactions.

In 2015, the restaurant industry is again at the forefront of a revolution in retail payments. This time, however, retailers (and third party providers) are attempting to shift consumer behavior away from the plastic card, to the consumer’s mobile phone device, as the payment initiation mechanism of choice. There are a number of reasons that retailers are pushing for this evolution in payment systems, including primarily the opportunities that “mobile payments” present for marketing and data mining. Most consumers already make mobile payments in a variety of forms, including online purchases on a mobile device, mobile banking and bill pay, peer-to-peer transfers, and mobile downloads and in-App purchases. Purchases at the physical retail point-of-sale are next, but consumers are not yet rushing to abandon their trusted plastic credit cards (or cash). According to the eMarketer research firm, about 16 million US shoppers used smartphones to pay for $3.5 billion purchases in stores in 2014, which is very small compared to the $4.3 trillion spent in stores overall in 2014 -- but significant growth is expected each year.\(^1\) Retail point of sale mobile payments will be marketed to consumers by parties like Apple, Google, PayPal, Starbucks, and LevelUp,\(^2\) who have already brought mobile payments to hundreds of thousands of retail locations. Retailers and franchisors considering how best to take advantage of this shift to mobile have no shortage of options, including upgrading point of sale hardware to work with an existing third-party services; building a proprietary solution in-house; or licensing a customizable, branded solution.

Whatever the choice of implementation, the progression to mobile payments will have far-reaching legal implications for retail businesses, and even more complex implications for franchise operations. Any retail business considering a mobile payment solution will need to plan out its approach to data collection, security, privacy, ownership and licensing of technology and intellectual property, consumer messaging and consumer protection compliance, and payments regulatory compliance. If the retailer selects one or more third-party vendors for its mobile strategy, the retailer will need to ensure compatibility across systems and consider indemnification for system downtime, consumer complaints, intellectual property infringement,

---


\(^2\) One of the co-authors of this paper, Brian Carroll, is General Counsel at LevelUp.
and sales tax consequences. Franchisors and franchisees seeking to roll out a coordinated mobile payments approach will face the same issues, but complicated further by the structure of their franchise agreements. This paper attempts to describe the current landscape for franchisors considering the adoption of mobile payment solutions.  

II. BACKGROUND  

A. Key Terminology  

The term “mobile payment” is now used in various circumstances to connote a variety of different transaction types and business models. For purposes of clarity, this paper will use these key terms as follows:

**Mobile Payment** – an umbrella term referring to any payment initiated, processed, or received using a mobile device (including for example “Peer-to-Peer Mobile Payments,” “Retail Mobile Payments,” and the other types of “Mobile Payments” discussed below and in Section II.D).

**Retail Mobile Payment** – payment initiated by a consumer to a retail merchant using the consumer’s mobile device at the physical, retail point-of-sale terminal, such as the checkout at a grocery or retail goods store, the counter at a quick-service restaurant, or table-side at a full service restaurant.

**Online Mobile Payment** – payment initiated by a consumer to a retail merchant using the consumer’s mobile device other than at a physical, retail point-of-sale terminal, such as through a mobile web browser, or for online food orders (i.e., order ahead or delivery).

**Peer-to-Peer Mobile Payment** - payment initiated by a user to another user (not a retail merchant) via the user’s mobile device.

**Mobile Payment Platform** – the infrastructure that enables the mobile-initiated payment, separate and apart from traditional payments networks (such as ACH, or Visa and MasterCard networks), banks, credit card processors, and point-of-sale hardware providers.

**Proprietary Mobile Payment Platform** - a retail mobile payment platform developed and used by a single retail brand.

**Private Label (or White Label) Mobile Payment Platform** - a retail mobile payment platform licensed to multiple merchants, each time customized to carry the particular merchant's brand, so that each merchant may offer a branded solution to its customers even though the underlying technology package may be basically the same.

---

3 Note that the laws governing mobile and online transactions, payment processing, data security, protection of personally identifiable information, etc. can all vary greatly from country to country. This paper will focus primarily on issues arising in the U.S. market.
Ubiquitous Mobile Payment Platform - a retail mobile payment platform widely available for use by any merchant, such as Square, Apple Pay, or Google Wallet, and not associated with a particular retail brand.

B. Existing Payment Methods

Until recently, retail consumers in the United States had essentially three options to initiate payments at the retail point of sale. As always, consumers still have the option to pay with good, old-fashioned cash. Cash transactions continue to account for about 30-40% of retail payments (slightly higher in food service). Those consumers that do not like to carry cash can initiate a transfer from their bank account with a check, cleared via the Automated Clearinghouse (“ACH”) network. Paper check transactions are becoming increasingly rare, and those that are made are typically processed electronically (the check can be scanned at the point of sale (“POS”) and entered as an electronic ACH transfer). Third, the retail consumer can initiate payment with a bank-issued, magnetic stripe card, either a deposit account linked debit card or a traditional credit card. This third method has also now expanded in the United States to include “chip-and-pin” credit card payments (using the EMV standard). \(^4\)

1. Cash (and electronic Stored Value)

Cash payments require no explanation. There are two types of cash-equivalent payments, however, that merit further discussion.

a. Stored Value (“Closed Loop”)

Retail merchants frequently offer consumers the ability to use one of the three traditional payment methods to purchase prepaid stored value, typically in the form of a gift card, that can be redeemed for a future purchase as the equivalent of cash. A retail merchant may also allow its customers to earn (rather than purchase) stored value, in the form of points, loyalty dollars, or credits, in connection with a purchase or series of purchases. These prepaid value and loyalty rewards programs are referred to as “closed loop” programs, because they are redeemable only at the issuing merchant, and can be used only for the purchase of goods and services (i.e., they cannot be transferred or redeemed for cash, except under certain state laws requiring balance refunds). A number of third-party providers and POS system providers offer services that support a “closed loop” network for the issuance of stored value cards and rewards cards by a single retail merchant.

b. Prepaid “Open-Loop” Cards

Another “cash-equivalent” option for consumers making retail point-of-sale payments is a general-purpose prepaid credit card. One commonly recognized example of this type of stored value instrument is the Visa “gift card.” Another example is the reloadable BlueBird card, jointly created by AmEx and Wal-Mart. These cards are a hybrid between cash and credit card payments. On the one hand, the cards require the consumer to make a pre-payment in to create stored value prior to the use of the card at the retail point of sale. When a user does make a purchase, the pre-paid balance associated with the card declines. On the other hand, the cards look, feel, and act like traditional credit cards, and they are typically accepted at any retail or online point of sale that accepts Visa, MasterCard, or AmEx. Because the cards can be used

\(^4\) See discussion of the EMV standard, Section II.B.3.c.
ubiquitously, across unaffiliated merchants, the cards are referred to as “open-loop” stored
value. Prepaid Open-Loop cards may carry a variety of fees, expiration dates, and other terms
depending upon the issuer of the stored value card.

2. **Direct Pay from Bank (Checks and eChecks)**

   The paper check is now largely a dinosaur at the retail point of sale, but it is not quite
extinct. Checks operate via the ACH Network (Automated Clearing House), which is the
primary means of moving funds between two bank accounts, *i.e.*, a consumer’s checking
account and a merchant’s operations account. Most merchants that accept checks no longer
accumulate paper drafts for deposit (at which point the bank would enter the transactions into
the ACH Network). Instead, systems now exist to scan the paper at the point of sale (or in a
merchant’s operations center) and use the acquired information, bank account number and
routing number, to initiate the ACH transfer electronically. Incidentally, this is also true of check
deposits at most ATM machines.

3. **Debit and Credit Card Payments**

   a. **Traditional Card Payments**

   Debit and credit card payments, which are now by far the most popular method of retail
point of sale payments in the United States (accounting for approximately 60-70% retail point of
sale payments), also come in a variety of forms. Visa and MasterCard are card brand
associations that offer networks enabling member banks (*e.g.*, CapitalOne) to issue consumer
credit cards, connected to credit accounts at the bank. These network cards are accepted
almost ubiquitously around the world. These networks are also used to process debit card
transactions, which are linked to a deposit account and require a PIN entry, for a variety of
member banks. Parties like American Express and Discover offer similar, but closed networks,
in which they act as both the network and the card-issuing bank.

   A credit card transaction at a retail point of sale involves a number of financial parties in
addition to the “issuing bank” that provides the consumer credit or debit card. When a consumer
presents a magnetic-stripe credit card at the retail point of sale, the merchant uses a device to
read the credit card number and other information from the magnetic stripe (or to manually enter
the information from the card). This point of sale device (provided by a vendor) receives the
consumer credit card information in plain text, and transmits the information to the merchant’s
payment processor (another vendor). The payment processor, working in connection with a
bank (known as the “acquiring bank”) provides the services necessary to submit the point of
sale transaction to the appropriate card brand network. The network routes the transaction to
the consumer’s issuing bank for authorization of the transaction. Assuming authorization, the
issuing bank later “settles” the transaction to the acquiring bank associated with the merchant’s
payment processor. The acquiring bank then makes a deposit into merchant’s transactional
bank account (typically at a third bank), after withholding the interchange fees for the transaction.

   b. **Interchange Fees**

   The term “interchange fees” refer to all the fees withheld from the retail merchant on
each transaction that are used to pay all of the parties that participate in the authorization and
settlement of a credit or debit card transaction. Most of the interchange fees collected by the
payment processor from the merchant is paid to the issuing bank. A smaller percentage of the
remaining interchange fees are paid to the card brand network (closed networks like American
Express collect both of these fees as network and card-issuer). The remaining interchange fees are split between the payment processor and acquiring bank. The merchant’s point of sale provider may also receive a per transaction fee. Interchange rates are established by the card brand networks (with pressure from large issuing banks), and vary based on a number of factors including the type of merchant (each merchant receives a Merchant Classification Code (“MCC”) from the card brand network), the type of credit card (certain rewards cards carry higher interchange fees than other cards), and whether the plastic card was presented to the merchant (“Card Present Transaction”) or not presented, such as in a phone or online order (“Card Not Present (CNP) Transaction”). The interchange fee is typically calculated by taking a set percentage of the transaction and adding a fixed, per transaction amount called a “swipe fee.” Unlike credit cards, interchange fees for debit cards were capped by federal legislation in 2010 called the Durbin Amendment, which capped interchange fees for non-exempt issuing banks (banks with over $10 billion in assets) at 5 basis points (0.05%) plus twenty-one cents ($0.21) per transaction.

c. **EVM and Chip-and-Pin**

The next step in the slow evolution of credit card payments in the United States market is the migration to the U.S., from Europe, of the EMV-standard (which stands for “Europay – MasterCard – Visa”), more commonly referred to as “chip-and-pin” cards or “smart cards.” The primary benefit of chip-and-pin card payments is security that the “chip” on the card enables encryption and dynamic authorization of the cardholder account information in a way that the traditional magnetic stripe does not. A “chip” card allows the point-of-sale device to process the transaction using encrypted card information, rather than plain-text card information read from a traditional magnetic strip. The chip also serves to prevent counterfeit magnetic stripe cards (created using stolen account information) from being used at retail point of sale terminals. In 2011, Visa announced that it would require merchants to upgrade to point-of-sale terminal hardware with chip-and-pin capability by October 1, 2015, or bear the risk of all future card-present, counterfeit credit card fraud (merchants currently have no liability for counterfeit credit card fraud if the credit card is present at the time of the transaction). Most merchants, however, have not rushed to make expensive point-of-sale hardware upgrades even in the face of the October 1, 2015 deadline.

C. **Alternative Payment Methods**

1. **Carrier Billing**

Outside of the United States, other point of sale payment services have emerged, offered by telecommunications network and service providers. This approach, referred to as carrier billing, enables consumers to make payments, including bill payments, Peer-to-Peer Mobile payments, and retail payments, to be charged directly to their telecom service provider bill. In many countries, carrier billing provides a form of banking service to the otherwise unbanked population. In the United States, where a high percentage of the population uses traditional banking services, carrier billing has been used primarily for digital content purchases on the mobile device. The first carrier in the United States to offer a physical point-of-sale purchase service is Sprint. In early 2015, Sprint launched an integration with LevelUp that

---

5 The Durbin Amendment became Section 1075 of the Dodd-Frank Wall Street Reform and Consumer Protection Act, and added Section 920 to the Electronic Funds Transfer Act (“EFTA”), codified at 15 U.S.C. §§ 1693 et. seq.
permits Sprint customers to charge purchases at the physical point-of-sale directly to their monthly Sprint bill.

2. Cryptocurrency

Another form of alternative payment capturing more than its fair share of recent press (and therefore demanding inclusion here for background) is cryptocurrency. The most widely recognized form of cryptocurrency is Bitcoin, although there are literally hundreds of other forms of cryptocurrency available. The fundamental technology of Bitcoin is the “block chain,” a digital record of all Bitcoin transfers, for all time, which is maintained and updated by a distributed set of independent computers. Although cryptocurrency can be exchanged for cash through a number of private (and still largely unregulated) entities, Bitcoin is not guaranteed or backed by any entity or government. The initial utility of Bitcoin was that it permitted users to make anonymous online purchases and transfers outside the regulated banking network (as an alternative to credit card or bank account transfers, that are traceable to an individual). The anonymity of Bitcoin is essentially the opposite of what most retailers desire in a mobile payment – a connection to the consumer. As governments begin to regulate Bitcoin operators, including by applying anti-money laundering regulations, the anonymity offered by Bitcoin begins to fade. Bitcoin may still survive as a cost effective alternative to Western Union for some international remittance transfers, but is unlikely to become an important piece of any retail mobile payment strategy.

D. Mobile Payments

As noted above, the term “mobile payment” is used to refer to a wide variety of consumer activities and technology providers that are as different as cash and credit cards. By late 2015, everyone has now associated the term “mobile payment” with ApplePay; just tap your phone to pay at a retail point of sale. But in reality, the term “mobile payment” has been around a lot longer than ApplePay (which was announced in September 2014) and generally refers to any payment that involves a mobile device. For example, a consumer might present a credit card at a farm stand or food truck to a merchant who swipes the card with a reader device plugged into an iPhone. A consumer with an Android mobile device might use the Citibank mobile App to pay a utility bill, or use the Amazon App to order diapers. An iPad user might pay for a parking spot while sitting on the train, or rent a movie through iTunes prior to a flight. All of these payments occur on mobile devices, and present their own advantages, disadvantages, and legal concerns. In classifying the various types of mobile payments, some of the key questions to ask are: (i) What is the payment credential and how is it presented?; (ii) Does anyone hold or store the payment credential or account information?; (iii) Who initiates the transaction?; (iv) Who receives data concerning the transaction?; and (v) Who has access to the account where the funds actually reside?

1. Mobile Card Acceptance Devices

Mobile card acceptance devices are hardware that plug into a standard smartphone or tablet, and are able to read magnetic stripe data from a traditional credit card swipe. These tools feed the magnetic stripe data into the phone or tablet, and enable the phone or tablet to operate like a point-of-sale terminal (and therefore provide security equivalent to that of a POS terminal). For a long time, Square (with its Square reader plugin device) was the standard for mobile card acceptance devices. Recently, however, Square faces growing competition from startup competitors, such as Shopify, and mobile-point-of-sale plays by more established competitors, such as PayPal Here, Amazon Local Register, and Groupon Breadcrumb. These payments are
Considered “mobile” payments, despite that fact that the consumer uses a traditional plastic card, because they are processed on a mobile device. The flexibility of mobile makes the payment solution popular at mobile retail locations, such as food trucks, or with other mobile service providers.

2. **Mobile Banking and Bill Pay**

Most major financial institutions now have some form of consumer mobile application that allows users to view and manage their deposit accounts, such as checking and savings accounts, from their mobile device. A number of these applications, such as the mobile banking applications from Chase, Wells Fargo, and Bank of America, enable consumers to make deposits by scanning checks using a mobile device, and to arrange for and make payments to third parties using the banks’ bill-pay service. These mobile-initiated bill payments, whether to utility providers, cellular carriers, or mortgage holders, are another form of “mobile payments.”

3. **Mobile Peer-to-Peer Payments**

With a number of notable exceptions (such as ClearExchange, Chase QuickPay, and PopMoney), most mobile banking applications do not easily permit transfers between consumer bank accounts at different banks (commonly referred to as a peer-to-peer payments). A number of third-party providers have solved that problem by allowing users to link bank accounts or credit cards and send money to friends using a mobile application, simply by entering a friend’s username, email address or phone number. The most established name in this market is PayPal. But a number of startup providers offer competitive services with lower fees, such as Venmo (which was acquired by Braintree in 2012 and is now a PayPal subsidiary), Dwolla, and Square Cash. Larger players, such as Facebook and Google, now also enable Peer-to-Peer Mobile Payments through their messaging and email services.

4. **Internet Commerce from a Mobile Device (and Online Ordering)**

Even prior to the proliferation of mobile smartphones and other mobile computing devices, a large portion of retail commerce had already migrated to the Internet. Most consumers are quite familiar with the concept of e-commerce, i.e., the use of traditional credit cards to make purchases from their home computers. Now, e-commerce is also available on a user’s mobile device. Most smartphones have full internet browsers that bring the traditional e-commerce approach to the mobile device, allowing consumers to enter their credit card (and shipping) information into a merchant website to make a retail purchase. In addition, a number of smartphone Apps, such as the Amazon App, enable consumers to input a credit card (or access an account with a card already on file) and make retail purchases directly within the application. These payments, though essentially just e-commerce transactions, are now “mobile payments” made from a mobile device.

The translation of e-commerce to the mobile world has also resulted in some new types of mobile payment applications (that also are effectively just e-commerce transactions on a mobile device), such as mobile parking Apps, like ParkMobile, and food ordering Apps (either for delivery or in-store pickup) like GrubHub, and Pizza Hut. Most people are also now accustomed to ordering, and paying for, car service or taxis via the Internet using Uber, Lyft, or similar mobile Apps.
5. Digital Content Purchases

Another popular manner of payment directly from a mobile device (and a dangerous method of mobile payment for anyone with children and an iPad) is payment through services that provide digital content to mobile devices. Digital content comes in many forms, including paid Apps or music through Apple’s iTunes or App Store, and Google’s Play channel, ring tones, content access subscriptions, gaming, or other in-App purchases. Payment for such content can be equally varied, and can be made through a payment account on file with Apple or Google, or often through a charge made directly to a phone service carrier bill.

6. Mobile Wallet

The “mobile payment” service making the most noise lately, and receiving the most press, is ApplePay. ApplePay, like its competitive predecessor Google Wallet, and the forthcoming Android Pay, is referred to as a “digital wallet.” ApplePay works by storing a tokenized form of the user’s credit card (or multiple credit cards) on the device in a “secure element.” If the user is paying at a retail point of sale device equipped to receive near field communication (“NFC”) from a mobile device, users can use their iPhone 6 device with ApplePay to transmit the tokenized credit card information into the point of sale terminal, as an alternative to swiping a plastic credit card. From the merchant’s perspective, this is no different than if the user paid with a traditional wallet and plastic card. The tokenized information is processed in the same manner as magnetic stripe data, through the merchant’s existing payment processor. As discussed below, this tokenization provides substantial security benefits over traditional magnetic stripe credit cards, in that the actual credit card number is not communicated to the POS device as plain text. This is sometimes referred to as “end-to-end encryption,” as the payment data is never transmitted in an unencrypted form. Further, in a digital wallet transaction, the merchant does not receive or store any information about the consumer.

7. Retail Point-of-Sale Mobile-Initiated Payments

As an alternative to a generic mobile wallet product like ApplePay, a number of other entities have launched retail point-of-sale mobile payment services that operate at least partially outside the traditional debit/credit card processing networks. The Starbucks App is the most high-profile example of a merchant-offered mobile payment solution (though the Starbucks App was initially a mobile stored value redemption product, addressed in the next sub-section). The Starbucks App allows a user to register via the App, link a payment instrument (such as a credit or debit card), and display a bar code within the App at the point of sale to initiate a payment. As discussed below, this approach provides an additional layer of security over a digital wallet approach in that the bar code or QR code does not encode any credit card information. Rather than passing the bar code information to its credit card processor directly, however, Starbucks uses the bar code identifier to retrieve the stored credit card information from the customer’s loyalty account, and then submits the transaction electronically to a payment processor. This extra step allows Starbucks to offer, and apply automatically, any customer loyalty rewards that the user has received before processing the transaction. Starbucks can also track an App user’s transaction history.

While Starbucks chose to build a Proprietary Mobile Payment Platform, a number of third-party providers have built (or have attempted to offer) mobile payment systems with out-of-the-box capability for customer tracking, engagement, and integrated rewards redemption within a mobile App. These mobile payment solutions come in a variety of formats, for example:
PayPal has included functionality in the PayPal App that enables PayPal users to make payments via PayPal at various small merchants that have PayPal accounts. The PayPal App requires a user to “check-in” via the App at a merchant location, which communicates the user’s identity information to the merchant. The merchant can then initiate a PayPal transaction (without credit card information) to the user’s account. In 2013, Square attempted to launch a similar solution aimed at small business merchants that used Square readers as a point of sale, but discontinued the service in 2014.

Merchant Customer Exchange ("MCX"), which is essentially a joint venture between some of the largest retail merchants in the country, including Wal-Mart, Best Buy, and CVS, is attempting to launch the CurrentC App, which was built by a provider called Paydiant (Paydiant was acquired by PayPal in 2015). The App, which has been in development for years, is now available for invitation-only testing. In previews released in 2014, MCX announced that the CurrentC App would work by enabling customers to use the camera functionality on their phone to scan a QR Code (identifying the merchant and purchase) for the transaction displayed by the merchant on a screen at the point of sale device. The user would then be able to complete the transaction using the phone and CurrentC App in communication with an MCX server (assuming a sufficient wireless signal was available) to convey the transaction information, the user’s payment instrument having been previously stored with MCX.

LevelUp, an independent startup company backed by investors including Google Ventures, developed a Mobile Payment Platform that enables any merchant to offer one-touch secure mobile payments with integrated customer rewards redemption, accrual, and tracking. LevelUp works by allowing a registered user to link a payment instrument and receive a QR Code (tokenization that does not encode any credit card information). When a user scans the QR code “token” at the point of sale (at a LevelUp scanner plugged into the point of sale device), the QR Code is passed directly to LevelUp, rather than the merchant’s payment processor. LevelUp is thereby able to apply rewards and track transactions prior to submitting the final charge to the user’s linked payment instrument. In addition to the LevelUp App, LevelUp also builds branded merchant Apps integrated to the LevelUp platform, including for brands like Steak ‘n Shake, Sweetgreen, Chop’t, Argo Tea, Protein Bar, and Organic Avenue.

8. Mobile Gift Card Redemption

As an alternative to the retail “mobile payment” Apps described above, other third-party providers offer mobile Apps that are designed to function as digital, reloadable gift cards. These Apps require a user to pre-pay stored value to the App provider, and permit the user to redeem the stored value at the retail point of sale by presenting a code (either a numeric code or a bar code) at the point of sale. These pre-pay Apps are often offered by entities that also provide traditional plastic gift card services, like Paytronix. As mentioned above, the Starbucks App was originally built strictly as a stored value redemption App. Other of the Apps mentioned above, such as PayPal, also offer stored-value pre-pay options in addition to the option for consumers to have their payment instruments charged in real time at the time of the transaction.
E. The Positives and Negatives of Retail Mobile Payments

1. Customer Convenience

It remains to be seen whether consumers really believe that a mobile payment is more convenient than a traditional credit card payment. Credit cards are simple, fast, and most importantly, familiar and comfortable to consumers. Mobile payments for retail, on the other hand, require a user to download software, register with a merchant or third party App provider, and link a payment instrument to a retailer and/or payment processor that they may not be familiar with. In some cases, like MCX’s CurrentC, the App may require complex user behavior at the point of sale (such as using a camera to scan a code displayed by the merchant and transmit the code to a third-party server), and the “check-in” and completion of the transaction depends on having a sufficient wireless connection.

If done correctly, mobile payment can provide a slick user experience and a “coolness” that also carries the benefit of increased convenience. Indeed, research indicates that acceptance of mobile payment can provide increased customer satisfaction by providing increased speed once customers are ready to pay, and increasing convenience because customers are not worried about finding a credit card, or making sure they have enough cash.\(^6\) When customers perceive that they have more control over a service encounter, they are more likely to be satisfied with that encounter.\(^7\)

In industries that see a higher percentage of payments by invoice and check (such as cleaning or homecare), mobile payments can provide a much higher level of increase in customer convenience, as well as lower risk of theft, fraud, and loss because of the greater security and traceability provided in the mobile environment.

2. Security

While “convenience” remains an open question, there is no question that mobile payment solutions generally provide a more secure means of payment. Services that tokenize the user’s payment credentials for transmission from a mobile device protect the user’s account information in a way that magnetic stripe credit cards, which convey the user’s actual (non-tokenized) credit card account number in clear text, cannot. Mobile payment services can eliminate the need for point of sale hardware to process account numbers in plain text, which has been a primary point of vulnerability for data breaches experienced by brands like Target and Home Depot. Consumers, however, may not yet understand the security benefits offered by mobile payments over plastic credit cards.

3. Branding

The shift to mobile payments for retail now offers merchants an opportunity they have never had — to issue their own branded payment mechanisms. Starbucks invested tens of millions to build a branded Proprietary Mobile Payment Platform so that customers would pay with the Starbucks App, rather than their plastic, bank-branded Visa card. Not all branded payment systems require that type of investment. For example, network providers like LevelUp now offer a branded payment App solution as a service, with significantly less capital expense.

---


\(^7\) Id.
Other entities, like Paytronix, offer branded mobile Apps integrated to a physical (plastic) gift card program, that permit users to purchase and redeem gift card (close-loop stored value) by presenting a code at the physical point of sale. These branded payment Apps not only grab space on the consumer’s phone, but also may slot directly into mobile wallet services like Apple’s Passbook and Google Wallet, right next to the user’s traditional cards, keeping the merchant brand top of mind.

4. **Consumer Data Collection**

The biggest benefit of mobile payments for retail merchants, by far, is the opportunity to engage with customers in a way that is impossible with credit card or cash payments. If done with a Proprietary Mobile Payment Platform or Private Label Mobile Payment Platform, the mobile payment experience allows the merchant to know the customer, to acquire data with each transaction concerning the customer’s purchasing habits, order patterns, location patterns, and in some circumstances, to track demographic information. Retailers can then use that data to market directly to the customer through the mobile payment App, or by email or other means.

Not only can marketing and promotion efforts become more targeted, but franchisors and franchisees are also able to receive verified information regarding the use and adoption of their loyalty programs. All rewards offered to the consumer through various channels become instantly trackable when claimed by the user and when redeemed at the point of sale through the mobile payment App. The consumer now becomes trackable across franchise locations, enabling brands to deliver promotions that more effectively increase the frequency of consumer visits and average spend.

Notably, these data acquisition benefits are not presently available in “mobile wallet” solutions like Apple Pay or Google Wallet, which provide the merchant only the equivalent of a credit card number and offer no opportunity for the merchant to acquire data about the user or transaction.

5. **Loyalty/Rewards Programs Adoption**

Closely related to data collection, mobile payment solutions allow merchants to integrate their loyalty and rewards programs (which otherwise would be implemented by separate plastic or paper cards) directly to the payment step. There is no longer any need for a two-step transaction in which the consumer presents a “rewards” card and then separately pays for the transaction by credit card. By combining the two steps into one mobile App, merchants can also drive much greater participation in their loyalty and rewards programs. By contrast, when a loyalty program requires that customers carry around a stack of paper or plastic punch cards, customers may be more selective about the programs in which they participate.

Implementation of a loyalty/rewards program into a mobile App carries the additional benefit (not only of trackability, as discussed above) but of security. Retailers no longer have to worry about “friendly fraud” on its loyalty programs (such as customers sharing loyalty punchcards, redeeming multiple single-use coupons, or abusing refer-a-friend campaigns), as mobile App-based loyalty programs are much less likely to be lost or counterfeited.

For franchisors, the introduction of a loyalty program and mobile payment system can provide a franchisor with direct access to end customers in ways that were never possible with paper based loyalty programs. For example, if a franchise location closes, the franchisor...
(assuming the appropriate consents were obtained) can retain access to customers in the area, and have a direct route to notify customers if a new location opens.

6. **Cost Savings/Check Increases**

For the retailer, especially in the restaurant and food service industry, implementation of an effective mobile payments strategy can both increase sales and decrease costs. Some mobile payment providers report data indicating that check sizes for restaurants increase up to 20% after adoption of mobile payment systems.⁸ For example, a consumer's restaurant spending typically increases 15% when the customer is redeeming a loyalty incentive.⁹ Even greater increased spend is observed when consumers are about to earn a loyalty reward (for example, a consumer will spend more to hit the $100 threshold and receive a $10 reward, and then will also spend more when redeeming the reward).

Similarly, retailers can save on transaction fees and risk of loss by implementing a “closed-loop” stored value program in connection with a mobile payments service, thereby decreasing the per transaction fees associated with credit cards. For example, the Starbucks mobile App allows customers to preload value into their Starbucks account in large amounts. So if a customer will spend $50 on ten cups of coffee, Starbucks can pay credit card fees once on a $50 reload, instead of paying high per transaction credit card fees on each of the ten five dollar cups of coffee. This kind of Mobile Payment Platform is not necessarily suitable for all franchise systems, but can be particularly useful for systems that rely on high frequency, low dollar value purchases.

7. **Targeted Messaging to Existing Customers**

Merchants that offer a mobile payment solution that enables data collection have the ability to contact users following the transaction, either directly within the App by push notification, or by other channels such as email or text (of course, as explained below, the merchant’s privacy policy must permit such activities). For example, a merchant can message all users who have visited in the past 30 days to announce a new product or service. Merchants can target specific groups of users (such as users who have not visited in the last two weeks) with individual promotions or rewards. Merchants that have a payment App loaded onto a user’s phone can now also utilize geolocation data, or “beacon” check-ins based on Bluetooth technology, to identify users in proximity to their retail locations and trigger specialized messages to the mobile App, or specialized rewards available for a limited period of time, to attract those nearby customers.

8. **Ability to Reach New Customers**

Driving increased sales from existing loyal customers that use a retail mobile payment App is important, but potentially more important is the ability to reach out to new potential customers who are users of a Ubiquitous Mobile Payment Platform. As noted above, “digital wallet” services like ApplePay and Google Wallet do not enable that type of marketing to users. A platform provider like PayPal, however, may offer the ability to reach all users of the mobile

---


⁹ Id. at 16.
payment service with special rewards offers, including users who have never visited a merchant’s locations.

9. Implementation Costs

Mobile payment services for retail vary widely in cost to the retail merchant, from ApplePay, which nominally costs the merchant no more than the cost of POS hardware to accept NFC credit card payments, to the Starbucks approach, which required millions of dollars of infrastructure investment. Because ApplePay is treated and processed as a traditional credit card payment, the merchant does not pay any premium with each transaction. ApplePay will, however, ultimately cost all merchants more for every “card-present” transaction (whether plastic credit card or mobile payment), because Apple will collect its fee from the interchange fee paid to the card-issuing bank for the transaction. The card-issuing banks will likely, in turn, force the card brand networks to raise interchange rates in order to offset the profits that issuing banks will begin losing to ApplePay.

Other providers of Mobile Payment Platforms and applications as a service may charge a variety of fees, including application and platform development fees, support fees, hardware fees for additional POS hardware and software, monthly hosting fees, and transaction fees.

In addition to the fees paid to a third-party provider, retailers and franchisors must also consider the internal costs associated with training staff and merging accounting systems and software, if necessary.

III. NEGOTIATION OF AGREEMENTS FOR RETAIL MOBILE PAYMENTS

Whether the franchise system is negotiating every aspect of the design, development and operation of a Proprietary Mobile Payment Platform, or reviewing a click-wrap license agreement in connection with a Private Label Mobile Payment Platform or Ubiquitous Mobile Payment Platform, there are many legal and business issues to keep in mind when adopting mobile pay platforms. As with so many new technologies, the law and practice are struggling to keep up with the market.

A. Deal Structure

Who will be the parties to which agreements? The first issue for a franchisor to consider is the range of services needed and the service providers to engage for those services. Some deals may involve several bilateral agreements to provide the products and services for a mobile pay system. For example, a merchant may sign a bilateral deal with a mobile pay vendor, and that vendor in turn may have a bilateral agreement with a payment processor for this particular merchant or for multiple merchants it services. Another approach would be to use a bilateral deal, with Master Services Agreement and Statements of Work for general projects. The service provider might subcontract out portions of the work or services, such as software development, online ordering or customer loyalty. In this type of situation, a concern arises when the “general contractor” chooses the “subcontractor”, but declines to take responsibility for the actions of the “subcontractor”. At a minimum any warranties and indemnities of the “subcontractor” should be passed through to the merchant.

Service providers also may enter into bilateral agreements directly with each franchisee or operator that will participate in the online Mobile Payment Platform, under terms dictated in the service provider’s agreement with the franchisor.
In some situations, more than two parties come to the table to enter into a multilateral agreement. The MCX agreement among participating merchants is an example of a multilateral deal.

Online terms for Ubiquitous Mobile Payment Platform such as ApplePay and Google Wallet are bilateral with users, but refer to third party agreements that also govern use of the mobile pay service: cardholder agreements, agreements with payment processors, agreements between card companies and banks, agreements with telephone carriers, and the like. In addition, the payment platforms’ terms state that the platform providers are not parties to the sales transaction between the consumer and the merchant.

Among the above may be agreements for a package deal that includes all the features a merchant seeks in a mobile pay system, or a la carte agreements for individual components of the mobile pay system such as app development for card storage and swipe, loyalty program, online ordering, feedback, customer relationship management (“CRM”), gift cards, menu disclosures, location beacons and check-ins, and more.

B. **Territory**

In what jurisdiction will the payment system be used? The legal and regulatory environment of the relevant jurisdiction, as well as consumer acceptance of different payment methods, should be a key consideration in choosing a platform. What is legal and accepted by consumers in the United States might not be legal or accepted in other jurisdictions. In the United States, franchisors should consider each of the items listed below.

C. **Development Agreement**

A development agreement to create a Proprietary Mobile Payment System will include the typical issues in any software or website development deal, including scope of work, specifications, design, user interface, interoperability and interface with other software/systems, milestones (lead time to launch), deliverables, acceptance testing, developers’ sandboxes, change orders, ownership, rights to use, fees and payment structure. These terms should take into account the overall context of the proposed use of the platform, what payment methods will be accepted, whether the system will handle iOS (Apple) and Android (Google) mobile devices, what POS hardware will be used, choice of payment processor and other vendors, and which party contracts with vendors, as well as the other terms discussed in this section.

D. **Hosting**

The mobile pay platform will need to be hosted on servers to make it available for use by consumers. A developer building a Proprietary Mobile Payment Platform might handle hosting duties, or a separate hosting service could be retained. Third-parties providing out of the box retail mobile payment services will also provide the platform support for the payment service. To support scalability and stability, and lessen the impact of failures and disasters, a hosting service may offer, or contract with, co-locator services that offer servers in different locations to run the platform software.

E. **Training**

The vendor may be required to provide training to the franchisor’s information technology (“IT”) team, or even individual franchisees. Training clauses could specify items
such as basic training; training on specific modules or features; train-the-trainer training; remote or in-person training; periodic training for new hires; number of training hours provided gratis; and rates for additional training.

F. Maintenance and Support Services

The agreement may have performance specifications relating to operational issues such as speed, load, and user experience. Maintenance and support services provided by the vendor typically involve 3 tiers of support, from routine handling of basic questions and issues by telephone and email for Tier 1, to sophisticated handling of complex failures for Tier 3, typically when Tier 1 and Tier 2 support have not resolved the issue. The vendor should be required to respond to questions and fix problems promptly, with the timing typically gauged depending on the severity of the problem. A merchant may provide Tier 1 support, and retain the vendor for only Tier 2 or Tier 3 support. Maintenance and support usually also includes providing bug fixes, updates, upgrades and new releases of software as they become available. In addition, the vendor should have and keep up to date a disaster recovery and business continuity plan.

Any negotiated contract should address each measurable area of the vendor's required performance with criteria to assess the success or failure of the performance. A service level agreement ("SLA") can address the minutiae of performance including speeds, load, scalability, stability (up time) and vulnerability, as well as availability of the platform and support. The SLA can provide for recourse for poor or failed performance with fee reductions, penalties or, in the extreme, termination rights.

G. Customer Service

Will the vendor answer questions and address problems not only from the franchise system's IT team, but also from consumers who use the Mobile Payment Platform? The agreement should address a range of issues concerning customer service and support, including hours of operation, scripts, answers to standard questions, escalation, qualifications and training of customer service representatives, specific security issues for customer service, languages, branding, upselling, outbound telemarketing, transfers to franchise system, reporting and auditing.

H. Bank/Credit Card Company Support

Generally, the mobile pay platform provider will interface with banks, credit card companies and payment processors, as well as provide receipts to customers, track transactions, check status of processing, and handle billing issues. Any agreement should address these types of services and support, with performance obligations. One also should consider possible interface with other vendors and service providers, such as for auditing, analytics and benchmarking.

Consider which party is responsible for chargebacks and review of transactions for possible fraud (despite heightened protection against fraud from tokenization that obscures credit card numbers).

I. Loyalty Programs

Loyalty programs may involve incentives to encourage adoption of the mobile pay platform as well as encouraging multiple visits to the store and purchases. Consumers may earn
loyalty points or credits by visiting a physical location and checking in (e.g., Belly), making a purchase (and the number of points may be scaled to the dollar amount of the purchase), or responding to an online or email marketing offer. Loyalty rewards might be in the form of special promotions, discounts, free items, free with purchase items, coupons or credits, which may be usable at the physical location, online or in-App. Some loyalty programs have added features, such as a shopping companion (price comparison, store locator, shopping list), identity storage and management, wish list, to do list, reminders (bill due, pick up milk, birthday gift), and friends’ gift lists.

Key to any loyalty program is the collection of personally identifiable data from consumers upon registration in the program and the opportunity to market to members with targeted messaging. Simple messages might be an email with a special coupon for a free item on the member’s birthday. Geofencing involves sending a message when the consumer is in certain physical location, such as entering a store, mall or neighborhood. Beacon messaging sends personalized, location-aware, application-specific messages, such as a specific message when the consumer downloads a particular App. Consumers also can be asked to participate in surveys or to try new products and provide feedback, to learn more about each consumer’s preferences.

J. Other Marketing Opportunities

Mobile pay platforms provide a host of other marketing opportunities. Typically each transaction involves an email and/or push notification receipt which may be sent to the purchaser via mobile device. The receipt is another opportunity to send a targeted message to consumers, such as by including an ad and a request for feedback.

In addition, a vendor may agree to provide ancillary marketing services, such as design and development of creative content, passing out flyers, online advertising placements, guerilla marketing (unconventional marketing), or email marketing services and management of suppression lists (lists of consumers who opted-out of receiving email marketing from the merchant). Many laws impact such marketing services (see Section III.V below), and vendor actions could lead to liability for the merchant as well. A merchant / franchisor that integrates advertising and marketing into its Mobile Payment Platform should be aware of federal and state marketing restrictions, as it should for its other advertising and marketing activities.

K. Data Reporting and Analytics

The primary benefit to retail merchants from a mobile payment system is the data and analytics the merchant can obtain. Point of sale data provides perhaps the most valuable data about customer purchasing behavior.

The service provider should be required to provide periodic or real-time reports, for example through a web-based data analytics interface, to the merchant with a range of data concerning use of the mobile pay platform and the merchant’s mobile pay App. However, that data viewed in isolation may be of limited value. Typically the service provider also is required to facilitate and engage on behalf of the merchant a data analytics company to review and report various metrics that help the franchisor understand and examine details about system performance and usage in context. Benchmarking against comparable programs may be valuable as well.
For example, Google Analytics is a web analytics service provided by Google to collect and store anonymous information about App users. Examples of the types of analytics provided by Google Analytics include:

(a) “Demographics and Interest Reporting” to analyze information regarding the interests and demographics of users.

(b) “Remarketing with Google Analytics” to place ads on other sites directed to site visitors.

(c) “Google Display Network Impression Reporting” to report how people’s interactions with the franchisor’s ads relate to their visits to the sites.

Google Analytics posts its own Terms of Use at http://www.google.com/analytics/tos.html; and its Privacy Policy at http://www.google.com/analytics/learn/privacy.html. Users may opt-out of Google Analytics for Display Advertising and customize Google Display Network ads by changing the ad settings, and may opt-out of being tracked by Google Analytics by downloading and installing Google Analytics Opt-out Browser Add-on for the user’s web browser. This information should be included in the franchisor’s Privacy Policy.

While the anonymous data provided by Google Analytics is interesting, retail merchants should be focused on identifiable data about its customers, to allow the merchant to engage with its customers at a personal level. A Mobile Payment Platform can provide the merchant with the ability to identify each registered App user (for example by name, email address, and dietary preferences) each time the user transacts. Use of Bluetooth or Bluetooth Low Energy (“BLE”) “beacons” permit the Mobile Payment Platform to identify the user when they walk by the store, or when they walk into the store. Using mobile payment Apps, merchants now know that Jane Smith (female, 29 years old, vegetarian) visits three of their locations at least once a week, usually on Tuesday at 12:30 pm, orders the kale salad 90% of the time, and 50% of the time adds a grapefruit soda. They also know that Ms. Smith walks by the 5th Street store every morning at 8:30 am and again at 5:30 pm. If Ms. Smith has linked a Facebook or other social account, the merchant may know that Ms. Smith has 15 friends that have also visited their stores in the last 30 days, and that she frequently visits the store with John Jones.

If the data is identifiable, the merchant can also track the effectiveness of marketing campaigns directed to individuals. For example, a merchant might try to encourage Ms. Smith to try one of their non-salad products, like a vegetarian soup, or to come in for breakfast rather than lunch. This offer can be conveyed through a personalized message to Ms. Smith received 10 minutes before she walks by the 5th Street Store each morning. The merchant can track not only Ms. Smith’s redemption of the offer, but also know if Ms. Smith returned to buy another soup or breakfast within the next 10 days. If Ms. Smith hasn’t returned to a store in 30-days, the merchant can send her a personalized offer to come back.

L. Fees

The fee structures for these types of services may be fixed, assessed based on time and materials (hourly or daily rates) for special projects, or subject to negotiation, depending on the nature of the services. Possible fees involved in these agreements could include fees for design, development, testing, hosting, co-location, hardware (e.g., POS systems purchase or leasing), support and maintenance services, transaction fees, gift card fees, advertising services,
administration of loyalty program, data analytics, conversion and set-up fees. The contract could specify periods of time with no fee increases, or caps on permitted periodic increases.

M. Intellectual Property Ownership, Protection and Licensing

Mobile payment systems may involve all areas of intellectual property ("IP"), including patents, copyrights, trademarks and trade secrets/confidentiality. For each area of IP, consider the following in contract negotiations:

1. **Patents**

   A patent is a property right in an invention granted by the federal government to an inventor. A patent may be granted to anyone who "invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvements thereof." Development agreements typically require assignment of inventions to the party that will be the ultimate owner of the Mobile Payment Platform. Joint ownership of patent rights is possible.

   In the case of a license agreement involving an existing mobile payment system that is protected by one or more patents which will be practiced by the licensee, the license agreement should specify that the licensee is granted a license with the right to make, have made, use, sell and import the subject matter of the patents.

   If the licensor’s patented technology provides a competitive advantage to the licensee, consider if the owner of the invention or patent should be required to prosecute patent applications and maintain issued patents, or at least to give the licensee the option to acquire ownership of any invention or application the owner chooses not to pursue, or any patent that the owner chooses not to maintain.

2. **Copyrights**

   Copyright protects original works of authorship fixed in a tangible medium of expression, by granting certain exclusive rights for a finite period of time. While inventive elements of software may be protected by patent, the software (including code and screen displays) also is protected by copyright. Development agreements should address which party will own the software that is created, including copyright and other IP rights, and require steps to ensure that the designated owner in fact acquires ownership of all copyrights. A common mistake occurs when a hiring party fails to obtain copyright assignments from its independent contractors, or describes the work of independent contractors as a “work made for hire” (which is unlikely to apply) without an express assignment of rights. Joint ownership of copyrights is possible, but the joint owners’ respective rights and responsibilities should be addressed in contracts to avoid uncertainty. Because copyright exists upon creation of the subject work, a copyright registration in the United States is not critical but can be helpful to document ownership and dates, and is mandatory to bring actions against infringers.

   A license to use a Mobile Payment Platform might include a copyright license for a downloadable App, or might be framed as remote access to the software through the cloud or other means of providing software as a service.

---

3. Trademarks

The types of trademarks at issue in a mobile pay system might include a word mark, design or logo, slogan or tagline, or the appearance and presentation of the system which, if non-functional and capable of identifying a single source of the system, may be treated as protectable “trade dress”. Examples include the brands Apple Pay™ and Google Wallet®, each applied to a mobile payment system. Along with the word marks are the familiar logos, and . Slogans could include “Shake to Pay” used by Starbucks or “Your wallet. Without the wallet.” used by Apple.

The key question is whose trademark (words and logo) will be used to brand and identify the Mobile Payment Platform. In the case of a Proprietary Mobile Payment Platform, or a Private Label Mobile Payment Platform (where the App or platform is licensed to multiple merchants, each time customized to carry the particular merchant’s brand, so that each merchant may offer a branded solution to its market even though the underlying package may be basically the same), the franchise system’s brand will identify the payment platform. The development agreement should specify the details of brand identity, including font, logo and color; where in the system the brand should appear, such as in the App, on receipts, and on email marketing campaigns; whether and where the vendor’s brand may be displayed; and the like. The brand owner / franchisor and the vendor will want to grant each other mutual, non-exclusive licenses to use their marks in the platform and related activities.

With a Ubiquitous Mobile Payment Platform, the platform’s brand (e.g., Apple Pay™) will be used and licensed to the franchise system with restrictions on the scope of permission to use the brand. The franchise system should explore when, where and how it may use the platform brand; the technical standards and format; and when the platform may change or update the brand, along with transition timing.

The key to trademark licensing is that a licensor must retain control over the quality of the licensee’s use of the mark. This is the reason behind clauses in contracts restricting trademark usage, requiring submission of samples for review, barring assignment of license agreements, and granting the licensor the right to terminate the licensee for failure to meet quality control standards.

In some instances, the parties may agree to a co-branding relationship that brands the payment system with both a merchant’s and a service provider’s brands. The franchise system may be allowed to use some combination of its brand with the platform brand. For example, the CurrentC App will be distributed by MCX, but co-branded in marketing for use at its member merchants like Wal-Mart and CVS. Co-branding can reinforce brands, through the association of the brands with each other, and may leverage marketing costs and exposure through shared resources and efforts. Some considerations in entering a co-branding deal include: how does the relative reputation and recognition of the proposed co-brand compare to your brand? Are the companies a natural fit in terms of products/services and markets? Do the parties agree on quality, customers, markets and channels of distribution? Have the parties participated in co-branding before, and what insights can be learned from that experience? What is the duration of the proposed co-branding endeavor, compared with set up and take down costs?
The risks of co-branding also should be considered: brand dilution, reduced control, and combining consumer perceptions that might be harmful if the co-brand has a recall or other adverse publicity. Considerations in the co-branding agreement may include exclusivity, committed funding for the program and its promotion, cost sharing, timing, territories and distribution channels, third party relationships, customer ownership, confidentiality, cooperation, performance metrics to measure success, term and brand usage guidelines.

4. Trade secrets and confidentiality

Trade secrets involve information that is the subject of efforts to maintain its confidentiality and that derives economic benefit from not being generally known. Information that may not qualify as a trade secret still may be deemed confidential information, and subject to contractual and fiduciary obligations to preserve confidentiality. Software and know-how concerning implementation of Mobile Payment Platforms may be protected as trade secrets and confidential information in development and other agreements. In addition, business parties to mobile pay agreements may have access to or develop information about another party's marketing plans, financial performance, personnel, vendor relations, customers and the like which may be protected under confidentiality clauses. Consumer data collected through use of the payment platform or loyalty programs may be considered trade secrets.

Confidentiality clauses (or separate non-disclosure agreements) should describe the general scope of trade secrets and confidential information, the standard of care in preventing or limiting disclosure to third parties, and a prohibition on use for any other purpose. To ensure enforceability of confidentiality clauses, in most states the practice is to expressly exclude from the confidentiality obligations, at a minimum, any information which is or becomes generally known through no fault of the receiving party.

Privacy Policies also will address the collection, use and handling of consumer personally identifiable information by different parties (see below).

N. Bankruptcy and Source Code Escrow

Software licensees and their businesses can be highly dependent on continuing access to the licensed software. Licensees should consider and address various possible reasons that the licensed software might no longer be available to them, including due to bankruptcy and pre-bankruptcy conditions. The bankruptcy code addresses some of these concerns, by providing that the licensee of a patent or copyright in an executory contract may elect to retain the licensed rights which a trustee in bankruptcy might otherwise terminate. This section provides some protection once the licensor is in bankruptcy, but leaves open concerns about obtaining support and maintenance for a retained license, further development, and the ability of a licensee to position itself when the licensor might be teetering on the verge of bankruptcy.

To address these concerns, licensees may require a software licensor to deposit the source code for critical software in a source code escrow with a neutral third party escrow agent. The licensor may be contractually obligated to provide the escrow agent with periodic updates so a current version of the code is always available. The parties may negotiate the conditions under which the escrow agent will be required to release the source code to the licensee ("release conditions"). Of course, the licensor will seek to limit the release conditions as much

as possible, while the licensee will try to obtain broader release conditions, such as if the licensor ceases to provide support and maintenance services, misses development deadlines, or fails to maintain the code to standards.

O. Data Ownership

A substantial amount of data may be collected through use of a Mobile Payment Platform, ranging from a consumer’s credit card number and personally identifiable information, physical location at a point in time (“geolocation”), usage information, financial information about the merchant, and aggregate performance and usage statistics. A wide range of additional information arises from a mobile payment system that includes a customer loyalty program, which might include customer identity, favorites, purchases, wish lists, email addresses and birthdays of customers’ friends and families.

Agreements pertaining to Mobile Payment Platforms and customer loyalty programs should specify the party (typically the merchant / franchisor) that owns each type of data, and what use rights, if any, are held by other parties to the agreement (franchisees, service providers) that may be involved in data collection, manipulation, use, storage or analytics. Payment method information (e.g., credit card numbers) typically would not be provided to the merchant / franchisor. All parties must handle and protect personally identifiable information pursuant to legal obligations (see regulatory discussion, below) and contract (including the applicable Privacy Policy, see below).

The service provider also should be charged with regularly reporting data collected concerning consumers who use the system, and either maintaining the data for the merchant / franchisor or making it available to the merchant / franchisor in an agreed format.\textsuperscript{12}

P. Data Handling, Storage, Security, Retention and Destruction

The agreement should set forth the vendor’s obligations concerning the handling of personally identifiable information in accordance with applicable laws, rules, regulations, guides, industry standards (including the PCI-DSS industry standards for credit card information discussed below), contracts and the Privacy Policy. As discussed further below, certain types of data are subject to specific regulatory schemes, such as financial information subject to the Gramm Leach Blilley Act; health care information subject to the Health Insurance Portability and Accountability Act (HIPPA) and Health Information Technology for Economic and Clinical Health Act (HITECH); and consumer information including credit information under the Fair Credit Reporting Act (FCRA).

The agreement also should require periodic security and penetration testing, including by a third party, and audit rights. In the event of a security breach, the agreement should address notice between the parties of a breach or suspected breach, and coordination and control concerning breach notifications and cooperation with state or federal regulators or law enforcement.

\textsuperscript{12} In Europe, a party must be designated as a data controller, the party who controls and is responsible for use of the personal information, or as a data processor, the vendor or contractor charged with handling the personal information, to identify their roles and responsibilities.
Q. **Open Source**

Not many years ago, software development deals and licenses expressly excluded open source software as antithetical to the long established notion of proprietary and confidential treatment of software code. As open source platforms and resources gained acceptance in the developer community, some of the concerns about open source have decreased. Open source software has the advantage of harnessing the broader development community to contribute ideas and further development, and to find bugs and help resolve problems.

Licensees should be aware that software designated by terms such as “open source,” “freeware” and “copyleft” is not necessarily “public domain” and freely available for use without restriction, but rather is subject to specific licenses with terms that should be reviewed and understood. These terms may disclaim all liability for IP infringement, require use of copyright notices, or require disclosure of proprietary software built on open source. Licensees of rights to use or access software that is open source or contains some open source components should seek warranties that the code is not subject to licenses that require disclosure of proprietary development, is non-infringing, and is not vulnerable to attacks and incursions. Another concern about open source is the possibility that the developer’s employer at the time of development will claim “shop rights” which create an implied license to the employer of a developer who invents the code on the employer’s time or using the employer’s facilities. This could enable the developer’s employer to claim either ownership or a right to use the software developed by its employee. For example, LevelUp’s software is mostly open source.

R. **Warranties**

Software licensors often seek to license the software “as is” with a disclaimer of all warranties. Licensee merchants / franchisors, on the other hand, seek a variety of warranties for protection.

One of the most important warranties is against infringement of third party IP resulting from authorized use of the licensed platform. The franchisor’s / licensee’s position would be that the software licensor has developed or acquired the licensed platform and should be in a better position than the licensee to assess whether the platform is likely to infringe the rights of a third party IP owner. The software licensor may counter by noting that infringement claims may arise unexpectedly despite its efforts to avoid them, that patent trolls may bring spurious litigation seeking settlements from deep pockets, or that the franchisor’s use of the system may go into fields or territories where the system has not previously been used and thus raise new issues.

A compromise approach might be for the licensor to warrant non-infringement in certain territories (such as the United States only, for an international franchisor), that no claims of infringement have been asserted to date, and that the licensor has no knowledge of any basis for such claims. The licensee may choose to conduct its own due diligence and make its own analysis of possible exposure to third party infringement claims. Sometimes an opinion is requested from the licensor, or from a neutral third party. Another alternative is to set aside a reserve for use in the event claims of IP infringement arise.

If the transaction is governed by the Uniform Commercial Code (“UCC”), a warranty of non-infringement might apply if not expressly disclaimed. Generally, the UCC applies to goods rather than services, although some cases have applied the UCC warranty of non-infringement
to commoditized or off-the-shelf software.\textsuperscript{13} In \textit{Rottner v. AVG Technologies USA, Inc.}, the company’s advertising claims were regarded as express warranties supported by language in the company’s end user license agreement ("EULA").\textsuperscript{14} The decision indicates that the more commoditized and generic the software, the more likely such software may be treated as a good rather than a service, at least under the Delaware UCC.\textsuperscript{15}

Most licensors seek to disclaim implied warranties, typically mentioning warranties of merchantability or fitness for a particular purpose in the disclaimer, but sometimes also including any warranty of non-infringement. Licensors also may disclaim that the mobile payment software will be adopted widely enough by consumers to be worthwhile, or to result in a profit for the merchant. Licensors also disclaim that the system will operate uninterrupted or error free.

Other typical warranties made by a software licensor include that the software was developed by appropriately trained developers performing in a workmanlike or commercially reasonable manner; that the software meets the specifications and will perform in accordance with the specifications for a certain time period; that the software is free from viruses and other unauthorized software that may interfere with the performance of the software or users' computers, or may provide backdoor access to the licensor or enable the licensor to cut off use; that the software complies with all applicable laws, regulations, rules and industry standards, ranging from employment law to export restrictions to privacy and data security; that the software is fully compliant with the Payment Card Industry Data Security Standards (PCI-DSS),\textsuperscript{16} the rules and guidelines of the credit card associations, and has been certified as compliant by a third party auditor; and that the system has not been the subject of any data breach or claimed data breach.

S. \textbf{Indemnification}

A merchant / franchisor that is a licensee of software or a Mobile Payment Platform typically will seek indemnification by the licensor against costs and expenses that may arise in connection with claims brought by third parties. As with warranties, a key area for indemnification is against claims for IP infringement. If the licensor granted a sufficiently broad warranty against IP infringement, the indemnification clause may simply state that the licensor will indemnify the licensee against any breach or alleged breach of warranty (picking up the full range of warranties). Some licensors prefer to disclaim warranties and specifically the warranty of non-infringement, and provide only an indemnification against IP infringement.

Licensors may seek to shift the risk of IP infringement (which can be costly) to the licensee by denying indemnification if the licensee uses the software or platform outside a selected territory (e.g., outside the United States) or with other products or programs that the


\textsuperscript{14} Id.

\textsuperscript{15} See also \textit{Surplus.com, Inc. v. Oracle Corp.}, 2010 WL 5419075 (N.D. Ill. Dec. 23, 2010) (software development agreement was governed by the UCC; although the custom software development involved the provision of services, the services were ancillary to the software that was the heart of the relevant agreement; applied UCC statute of limitations). Compare \textit{Digital Ally, Inc. v. Z3 Technology, LLC}, 2010 WL 3974674 (D. Kan. Sept. 30, 2010) (in dispute over development of custom modules, court held that a pure license agreement does not involve transfer of title and so was not a sale of goods under UCC).

\textsuperscript{16} See Section III.V.3.a., below.
licensor did not approve for use with the licensed software or platform, or if the licensee modifies the software or platform other than through the licensor. Licensors also may seek to limit their exposure with exclusions for indirect and consequential damages, and limitations on liability. In addition, licensors may include language giving themselves the right to mitigate damages from a possible infringement by modifying the platform, obtaining a license for substitute non-infringing elements, or terminating the license if neither of the two prior alternatives is viable.

Beyond indemnification for the licensor's breach of warranties, other typical indemnification clauses may cover the licensor's or its contractors' breach of the agreement or violations of applicable law; claims arising from licensor's agreements or relationships with third parties; and damages caused by the licensor's or its affiliates' fraud, willful misconduct or gross negligence.

Indemnification clauses for the licensee merchant / franchisor similarly may include breach of warranties, breach of agreement, violations of law, misuse of any user data acquired from a licensed platform, failure to honor any campaign reward or credit, failure to maintain POS integration to meet the licensor's requirements, physical injury or property damage caused by franchisor or its goods or services, misuse of the platform by franchisees, and claims based on the franchisor's changes to source code or infringement caused by IP provided by the franchisor.

Indemnification clauses for a franchisee / operator entering into a direct agreement with the licensor may include indemnification for breach of warranties, breach of the agreement, violations of law, misuse of user data, failure to redeem campaign incentive or reward or credit, or any physical injury caused by operator or its goods or services in connection with the mobile pay platform.

For licensors that might not have the resources to cover indemnification exposure against IP infringement or other claims, licensees may seek to require that the licensor carry certain types of insurance to fund some or all possible exposure from IP infringement claims and other indemnification obligations, and to be added to the licensor's insurance policy as additional insureds.

T. User Agreements

1. Privacy Policy

The agreement should address which party interfaces with users in the collection and use of personal information, and which party's privacy policy will be posted to govern user interactions. The privacy policy is essentially a binding statement to consumers concerning the company's privacy activities. FTC guidelines and California laws such as the Shine the Light Act and the Do Not Track Law, among other regulatory compliance issues (see Section III.V below), should be addressed in privacy policies. Responsible parties should contractually impose compliance with the privacy policy on their vendors.

For the Ubiquitous Mobile Payment Platforms, Apple Pay does not have a separate Privacy Policy, but is governed by the Apple Customer Privacy Policy, Apple's general privacy policy. Apple Pay posts an overview of the security and privacy issues in the general privacy policy. Google Wallet similarly is governed by the general Google Privacy Policy but that is supplemented by the Google Payments Privacy Notice which contains additional information about what is collected and additional ways in which such information is used.
2. Terms of Service / Terms of Use

Similarly, the website terms of service or terms of use should be posted by the party in the direct relationship with users. The terms form a contract with users that may address, among other things, limitation of liability concerning the website or App, ownership of IP, user generated content, and other details concerning use of the website, App or service. Like privacy policies, the terms should address a number of additional legal issues, some of which are discussed in additional detail below in Section III.V.

Level Up’s Terms of Service and Google Wallet’s Terms of Service are agreed to by the user when registering an account through the App. Both Terms of Service provide that use of the service signifies the user's authorization to charge the user's payment instrument. The Apple terms provide that by using Apple Pay, the user agrees to the collection, maintenance, processing and use of the user's information to provide the Apple Pay functionality. The Apple Pay Supplemental Terms and Conditions are included with the software license agreement agreed to by users in connection with downloading iOS for their Apple phones or OS on their Apple Watches.

Terms of Use also may include similar disclaimers to those made by software licensors, but are likely to be even more one-sided, including disclaimers for all implied warranties including non-infringement, that the software is free from viruses or errors, etc., as well as disclaimers for liabilities in connection with purchases, payments or commerce activity using the mobile pay platform.

U. Americans with Disabilities Act

Some cases and enforcement actions have required online services to comply with the Americans with Disabilities Act (“ADA”) to be accessible to those with physical limitations. This is a developing area that may impact mobile payment systems.

The Ninth Circuit recently ruled that a website-only business (with no physical location open to the public) is not subject to the ADA. The Ninth Circuit apparently is the first federal circuit to decide this issue as it relates to website-only businesses. In reaching its decision, the Ninth Circuit relied upon its earlier case holding that a long-term disability insurance plan was not a “place of public accommodation” and thus not actionable under Title III of the ADA.

The circuits seem to be split on whether Title III of the ADA applies to businesses without retail physical locations (e.g., insurance companies), and it remains to be seen how those circuits would rule on the issue of website-only businesses or Mobile Payment Platforms. District courts in Vermont and Massachusetts have a broader interpretation of the ADA than the Ninth Circuit and have held that website-only businesses are subject to ADA.

17 See Earl v. eBay, Inc., 599 Fed. Appx. 695 (9th Cir. 2015) (affirming dismissal because eBay's services are not connected to "an actual physical place"); Cullen v. Netflix, Inc., 600 Fed. Appx. 508 (9th Cir. 2015) (affirming dismissal because Netflix's services are not connected to "an actual physical place").

18 Weyer v. Twentieth Century Fox Film Corp., 198 F.3d 1104 (9th Cir. 2000).

The Department of Justice (DOJ) actively enforces ADA compliance with respect to physical locations, websites, mobile Apps and other technologies. It has targeted some high-profile companies, including Wells Fargo in 2011 (with respect to its website among other things), and Peapod in 2014 (with respect to its website and mobile applications), and EdX in 2015 (with respect to its website, mobile applications, and open source learning platform). Notably, Peapod’s and EdX’s services are offered only online. In May 2015, the DOJ moved to intervene in a blind student’s ADA suit against Miami University, to focus on accessibility of the university’s technology and website. Franchise systems are not immune from ADA enforcement actions if the systems they adopt fail to comply with ADA requirements.

The DOJ has announced a planned release of new regulations relating to website compliance with Title III of the Americans with Disabilities Act, but the release date has been moved back several times. The new release date is anticipated to be no earlier than April 2016.

V. Compliance with Laws and Regulations

A franchise system adopting mobile payments should be aware of the massive web of state and federal laws that may be relevant to mobile payments and other types of mobile marketing programs. Whether developing a Proprietary Mobile Payment Platform, licensing a Private Label Mobile Payment Platform, or adopting a Ubiquitous Mobile Payment Platform, a merchant or franchisor must be extremely careful to understand the regulatory requirements and how those regulatory requirements may apply to its mobile payment offering.

Laws and regulations governing or affecting mobile payments come from a variety of different sources, including:

1. Financial Laws
   a. Banking Regulators (Federal Reserve, FDIC, OCC, NCUA)

   If a franchisor is acting in a banking capacity, a number of banking regulators may have jurisdiction to regulate its activities. The Federal Reserve, the Federal Deposit Insurance Corporation (“FDIC”), the National Credit Union Administration (“NCUA”), and the Office of the Comptroller of the Currency (“OCC”), all have regulatory authority over entities operating in a banking capacity.

   Since franchisors interested in mobile payments do not need to establish a bank, banking regulators should play a limited role in a franchisor’s mobile payments strategy. Regulation by the federal and state banking authorities, if any, should be the concern only of the vendor engaged to build or operate a mobile payment system. A franchisor building a Proprietary Mobile Payment Platform, and holding prepaid value only usable for the purchase of consumer goods and services, should have no concerns.

---


With regard to a loyalty program, banking regulations would not apply if the entity issuing the gift cards is the same entity that provides products or services purchased by those cards. However, in the typical franchise system, one franchisee (or the franchisor) might issue cards, while a different franchisee might provide the products or services. Although the authors are not aware of current enforcement by federal and state banking regulators regarding these intra-franchise systems transfers, the existing rules do not clearly exempt franchise systems.

b. State Licensing of Money Transmitters

Forty-seven of the fifty states regulate “money transmission” in some form. Although state laws differ, in some cases markedly, the laws are generally drafted to require registration and licensing by any entity that moves money between a payor and payee, such as a consumer and a retail merchant. State regulators generally are familiar with franchising and treat the franchisor and its franchisees as one entity. A mobile payment vendor to a franchise system may be viewed a sufficiently distinct to be governed by these laws.

These laws also generally extend to require licensing for prepaid and stored value systems, such as gift card systems. These state statutes generally, but not always, exclude retail merchants offering their own in-house solutions and gift cards. But the exclusions do not always extend to a merchant’s vendors. Any entity building or contracting with a third party to provide or build a mobile payment solution will need to ensure compliance and appropriate licensing under the various money transmitter statutes.

c. Gift Card Laws

Many states have gift card laws that govern the issuance and acceptance of gift cards. State gift card regulations include required disclosures, restrictions on expiration dates and fees, requirements for providing refunds of small balances, and laws governing when abandoned funds (or breakage) escheat to the state.

Regulation E implements the gift card provisions under the federal Card Accountability Responsibility and Disclosure Act of 2009 (“Credit CARD Act”). The rule applies to gift certificates, store gift cards, and general use prepaid cards, as those terms are defined in the Credit CARD Act, but not other types of prepaid cards, such as reloadable prepaid cards not promoted as gift cards, and prepaid cards received through a loyalty, award or promotional program. The key provisions bar expiration dates before five years after purchase or after money was last loaded on the card; and inactivity fees before one year after purchase, and then no more frequently than once per month. The expiration date of a card must be clearly disclosed on the card itself, and any applicable fees must be clearly disclosed on the card or its packaging.22

In addition, the Consumer Financial Protection Bureau (“CFPB”) has issued proposed regulations relating to gift cards under the Electronic Fund Transfer Act.23 The stated purpose of the proposed rule is to “expressly bring [prepaid financial products] within the ambit of Regulation E as prepaid accounts and create new provisions specific to such account.”24

---


24 Id. at 1.
Proposal states that the rules would “establish disclosure requirements specific to prepaid accounts that would require financial institutions to provide certain disclosures to consumers prior to and after the acquisition of a prepaid account.”

d. **Consumer Financial Protection Bureau**

The CFPB, created in 2011, is charged primarily with responsibility for enforcing the Electronic Funds Transfer Act (“EFTA”) and Regulation E, and the Truth in Lending Act (“TILA”) and Regulation Z.

Regulation E governs all parties engaged in transfers of funds initiated in a retail point of sale transaction, including merchants, payment processors, card issuers, and any other party providing a mobile payment application.\(^{26}\) The rules are directed primarily to receipts and billing practices, disclosures, consumer liability for fraudulent charges, and dispute resolution; and requirements for expiration dates and fees on gift cards and other prepaid stored value products (see above).\(^ {27}\)

Regulation Z (the regulations implementing TILA, enforced by the CFPB) is directed to “financial institutions” that extend “credit.”\(^ {28}\) However, the scope of the regulations is expansive as a consequence of the broad and vague definitions of those terms. In general, the regulations are primarily directed to institutions that charge consumers a fee for a payment service. Most mobile payment systems do not charge any fee for use, making Regulation Z largely inapplicable. Depending on the implementation of a merchant’s mobile payment approach, however, merchants may need to ensure compliance with the full extent of Regulation Z. Even where no consumer fee is charged, Regulation Z imposes certain disclosure requirements upon mobile payment providers.

e. **Financial Crimes Enforcement Network**

The Financial Crimes Enforcement Network (“FinCEN”), a division of the Treasury Department, governs Money Services Businesses (“MSB’s”), and enforces the Bank Secrecy Act. The Federal “MSB” designation is similar to the state designations of “money transmitter.” FinCEN focuses on controlling money laundering activity and the funding of terrorism. States, by contrast, are more concerned with consumer protection. FinCEN’s regulations implementing the Bank Secrecy Act are referred to as Chapter X, and include among other things requirements that entities providing mobile payment services maintain adequate anti-money laundering (“AML”) policies.\(^ {29}\)

\(^{25}\) id.


\(^{27}\) See Section III.V.c.

\(^{28}\) 12 C.F.R. § 226.1 et. seq. (2015)

\(^{29}\) 31 C.F.R. §§ 1010.100-1060.800 (2014).
f. Gramm-Leach-Bliley Act – Safeguards Rule and Data Privacy Rule; and State Law Equivalents

The Gramm-Leach-Bliley Act (“GLBA”) has two major components – the Financial Privacy Rule and the Safeguards Rule. The former imposes requirements on any financial institution that collects and stores Non-Public Information about a consumer. The Financial Privacy Rule imposes obligations on financial institutions requiring disclosure of how consumer personal information, called “Nonpublic Personal Information,” is used and shared. GLBA’s scope is limited to “financial institutions” and should not apply to retail merchants, but the provisions likely do extend to any party offering a mobile payment service.

GLBA is primarily enforced by the FTC in accordance with FTC regulations. The Safeguards Rule requires governed financial institutions to have a comprehensive written information security policy in place to protect consumer information. The Safeguards Rule does not include extensive specific requirements that must be included in the written information security policy, but it does include general requirements including designating an employee responsible for the program, conducting risk assessments, implementing measures to control identified risks, vendor oversight and continuous monitoring and improvement. Practically speaking, compliance with PCI-DSS for cardholder data will comply with the Safeguards Rule. However, the scope of PCI-DSS is limited to cardholder data, while the Safeguards Rule extends to the broader set of data defined as Nonpublic Personal Information. For this reason, PCI-DSS compliance alone is unlikely to meet all of the obligations under the Safeguards Rule.

The FTC’s Financial Privacy Rule sets forth very specific requirements for privacy policy disclosures, including the timing and frequency of such disclosures. The FTC, in partnership with the Securities and Exchange Commission, Commodity Futures Trading Commission, Consumer Financial Protection Bureau, Federal Deposit Insurance Corporation, National Credit Union Administration, and Office of the Comptroller of the Currency cooperated to release an interagency form notice for the Financial Privacy Rule, in 74 Fed. Reg. 62890 (Dec. 2009). In any situation in which both a franchisor and its mobile payment vendor are collecting consumer information through a mobile payment App, the parties will need to work together to ensure that consumers understand any differences in the scope of the applicable privacy policies.

g. FTC Red Flags Rule

The FTC Red Flags Rule requires financial institutions and some creditors to monitor transaction activity for behavior indicative of identity theft and to administer an identity theft prevention program. FTC’s Red Flags Rule is based on section 114 of the Fair and Accurate Credit Transactions Act of 2003 (“FACTA”). It is unclear whether mobile payment providers would be considered a financial institution or the type of creditors that would need to comply with the FTC Red Flags Rule. However, franchisors should ensure that any mobile payment vendor complies with relevant regulations.

h. EMV Chip Cards - Changes Concerning Fraud

On October 19, 2014, President Obama signed an executive order to speed adoption of EMV chip cards in the United States, with a deadline by October 1, 2015 (as described in Section II.B.3.c. above). The shift to EMV chip cards in the United States is likely to increase

---

the use of mobile payment for several reasons. First, when merchants upgrade their POS devices to allow for the new EMV technology, they may choose to upgrade to allow for mobile payment as well. Second, EMV chip cards are more expensive than magnetic stripe cards, which may cause issuers to push consumers toward existing or new mobile payment options. Third, one of the selling points of mobile payment technology is its ease of use and reduced payment time at the POS. In contrast, EMV technology requires leaving the card in the POS reader until the receipt prints. This “inconvenience” may increase payment time at the POS which customers may believe means EMV is less user friendly than magnetic stripe cards, which could increase the appeal of mobile payments.

2. Consumer Protection

   a. FTC Section 5 of the FTC Act

           Section 5 of the Federal Trade Commission (“FTC”) Act makes unlawful any unfair or deceptive acts or practices in or affecting commerce.

           The FTC's broad Section 5 powers have been used to pursue companies that have violated their privacy policies. If a merchant's privacy policy fails to disclose the information it collects about consumers online or how it uses that consumer information or otherwise breaches its privacy policy, the FTC may view this as consumer deception in violation of Section 5. The current structure of mobile payments shifts the responsibility of collection/use of data and necessary disclosures in privacy policies. Rather than a merchant's privacy policy governing the data collected in connection with the transaction, consumers will likely be storing sensitive data on their mobile device or mobile payment App and that information will be shared with the manufacturer of the device or App developer. Accordingly, privacy policies of device manufacturers and App developers will become more critical and subject to more FTC scrutiny.

           The FTC's Section 5 powers also have been used to pursue companies that have conducted marketing and advertising that it has found to be unfair or deceptive. Material representations (taking omissions into account) must be truthful and non-deceptive, and must not mislead consumers. The merchant should have support and substantiation for all material claims concerning a mobile pay platform as elsewhere in its business.

           In Federal Trade Commission v. Wyndham, the FTC went even further and brought suit claiming that a franchisor’s alleged failures to maintain reasonable security measures constituted unfair and deceptive practices under Section 5 of the FTC Act. The specifics of the FTC’s allegations illustrate the various ways in which liability can arise when franchisors impose specific technology requirements on their franchisees.

           The Wyndham computer system was a fairly typical franchise computer network. According to the FTC, Wyndham required that each Wyndham franchise location, and any other “Wyndham” branded property “purchase and ‘configure to their specifications’ a designated computer system that, among other things, handles reservations and payment card transactions.” At the time of the conduct at issue, that system stored various personal information including names, addresses, e-mail addresses, telephone numbers, credit card numbers, expiration dates and security codes. All of the computer systems at franchise

---

locations were also linked to the Wyndham corporate network, which allowed information to be shared through the system to coordinate reservations and payments.

The FTC claimed that the franchisor failed to employ commonly used methods of data protection. Specifically, the FTC claimed:

- Wyndham failed to adequately inventory the computers connected to the Wyndham network, which precluded Wyndham from adequately assessing and appropriately managing the devices.
- Wyndham failed to use firewalls or other security measures to limit access between various locations and systems, thereby allowing intruders to gain access to a number of different servers by breaching just one.
- Wyndham failed to require complex IDs and passwords, leaving the system vulnerable to brute force attacks.

From the FTC’s perspective, these failures were sufficient to make the franchisor culpable for data breaches that occurred in its system. Wyndham has challenged the FTC’s authority to regulate business data security practices, particularly in the absence of formal regulations. However, if the FTC is successful, franchisors may be federally liable if they fail to protect (and to ensure that their franchisees protect) customer data. Although it may be some time before a court rules on merits of the FTC’s claims against Wyndham, franchisors should be sure that both their own internal practices and the practices of any outside vendors are consistent with current data security best practices.

b. **Unfair, Deceptive or Abusive Acts and Practices**

Through the Dodd-Frank Act, Congress expanded Title 5 of the FTC Act to prevent certain “covered persons or service providers from committing or engaging in an unfair, deceptive, or abusive act or practice under Federal law in connection with any transaction with a consumer for a consumer financial product or service, or the offering of a consumer financial product or service.” Specifically, the Dodd-Frank Act added the standard of “abusive” to the existing “unfair” and “deceptive” standards in Title 5. Under the Dodd-Frank Act, the CFPB is authorized to issue regulations designed to prevent unfair, deceptive, or abusive acts (“UDAAP”).

c. **Controlling the Assault of Non-Solicited Pornography And Marketing Act**

When engaging in promotional e-mail communications, caution must be taken to comply with the federal Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003 (“CAN SPAM Act”). Among the CAN SPAM requirements, commercial emails must identify the message as an ad, not use deceptive subject lines or misleading to/from information, and

---


provide recipients with an opt-out mechanism. Note that the CAN SPAM Act states that an advertiser may not contract away its liability for violations of the CAN SPAM Act by hiring a vendor to send the messages.

d. **TCPA**

Prior to incorporating any promotional text messages or faxes into advertising and marketing, affirmative consent is needed from consumers. For example, in *Agne v. Papa John’s International, Inc.*, 286 F.R.D. 559 (W.D. Wash. 2012), a class of Papa John’s customers sued Papa John’s franchisees and the franchisor in connection with unsolicited promotional text messages sent by a third-party vendor. The Plaintiffs alleged that Papa John’s was responsible because it approved and encouraged franchisees to contract with the vendor for such services. News reports indicate that Papa John’s eventually paid $16.5 million to settle the case. However, franchisors will generally only be liable if it can be shown that the sender of the message was an agent of the franchisor. For example, in *Thomas v. Taco Bell*, Taco Bell successfully argued that it should not be held vicariously liable for a text message campaign that violated the TCPA. An association of franchisees had independently developed the promotions, and contracted with the vendor that actually sent the text message.

e. **Menu Disclosure Requirements**

In December 2014, the Food and Drug Administration issued a final rule regarding required disclosures on menus and menu boards in restaurants and similar establishments. Effective December 1, 2016, all covered establishments will be required to (a) disclose calories for standard menu items on menus and menu boards, (b) ensure that written nutrition information for standard menu items is available to consumers who ask to see it, and (c) include a statement on their menus advising consumers about the number of calories that should be consumed daily. Importantly, for purposes of this paper, the term “menu” is intended to cover any menu available to customers while they are placing orders. The regulation specifically provides that the term “menu” includes electronic menus and menus on the Internet. If a mobile App allows electronic ordering, then it will be subject to the calorie disclosure requirements.

Moreover, “covered establishments” specifically includes independently owned franchises if there are 20 or more locations in the franchise system. Very few of the existing

---


42 21 C.F.R. § 101.11(a) (2015) (“covered establishment means a restaurant or similar retail food establishment that is a part of a chain with 20 or more locations doing business under the same name (regardless of the type of ownership, e.g., individual franchises”).
regulations requiring calorie counts on menus provide specific guidance for display of that information on mobile devices. However, in practice App developers have met these requirements by including nutritional information in the App and allowing links to particular food items to expand to show any required nutritional information.

f. Guidance Regarding Mobile and Electronic Disclosures

In recent years the Federal Trade Commission has provided guidance regarding various electronic disclosures. The FTC’s recommendations for disclosures in digital advertising are instructive for developers of Mobile Payment Platforms. The guiding principle is that disclosures must be clear and conspicuous from the perspective of a reasonable consumer. The disclosures must be prominently displayed in plain language, in close proximity to the claim that the disclosure is qualifying, and technological limitations must be considered to ensure that all users receive adequate disclosure regardless of the platform they are using to access the information. Recognizing that required disclosures may be challenging on a small screen, the FTC has also provided guidance for effective disclosure specifically in mobile environments. Best practices including having a privacy policy that is easily accessible; providing “just-in-time” disclosures; obtaining affirmative consent before allowing Apps to access sensitive information such as geolocation, contacts, and photos; and investigating all third-party code and third party services that integrate with the App so that all consumer disclosures are accurate.

3. Industry Standards / State Statutes

a. PCI-DSS

The Payment Card Industry Data Security Standard is an information security standard for the protection of cardholder data. PCI-DSS was developed and is maintained by the PCI Security Standards Council, which consists of representatives from credit card industry companies including the major card companies Visa, MasterCard, American Express and Discover. Information about PCI-DSS may be found at www.pcisecuritystandards.org.

To comply with the requirements of PCI-DSS, it is important to consider which parties will have access to credit card data. Contractual obligations are needed from each such party that it is in compliance with, and will remain in compliance with, PCI-DSS, with audit rights or third party verification, as well as indemnification or other risk-shifting provisions to protect the merchant should the vendor have a breach. When using a Mobile Payment Platform provider (which transmits encrypted information), the data will be held by the provider and not the merchant. However, a merchant accepting credit cards in the traditional fashion holds unencrypted credit card numbers and is responsible for proper handling of that data.


44 Id.


46 Id. at ii-iii.
Because PCI-DSS requires franchisors to assess and comply with PCI-DSS standards for all systems that are connected to any database in which payment card information is processed or stored, the cost and scope of PCI-DSS compliance also varies based on the connectivity of a franchise system. In the typical franchise system, customer payments to franchisees are processed by the franchisees, and customer payments to the franchisor (e.g., for company-operated locations) are processed by the franchisor. If the two systems function completely independently, a franchisor can easily meet its PCI-DSS obligations without regard to its franchisees’ systems, and vice versa. However, as the franchise model and technology evolve, more and more franchisors are connected to their franchisees’ management systems to provide remote management services, administer loyalty programs, provide centralized reservations, validate receipts, or allow franchisees to connect to the franchisor intranet. In some franchise models, and in some Mobile Payment Platform structures, the franchisor or a third-party vendor may actually process credit card payments on behalf of its franchisees. Each layer of connectivity can add to the scope of the franchisor’s PCI-DSS compliance obligations, the costs associated with compliance, and the scope of its potential liability.47

b. **State Laws on Data Breach Notification and Data Security**

At least 47 states and several territories have established laws requiring notification of individuals whose personal information is compromised in a data breach. Generally speaking, these laws require businesses that own or license personal information to notify state residents if their information is compromised. The laws are largely similar, but vary in certain details such as the definitions of personal information and breaches, timing of notification, and whether state regulators must be notified of the breach. The notifications in some states must contain specified information and must generally occur without unreasonable delay after the breach is discovered. Where notifications to regulators are required, they typically must occur prior to or no later than the time when residents are notified.

Several states have implemented laws that govern organizations that collect and use personal information from the states’ residents. These laws include both general laws and laws specific to payment card information. At least three states have adopted laws specific to the protection of payment card information, with two specifically converting PCI-DSS requirements into legal obligations. Most prominently, Nevada law requires merchants doing business in the state to comply with PCI-DSS.48 In addition, Washington state law provides a cause of action for financial institutions for breaches of card information if the merchant does not take reasonable care to protect card information, but includes a safe harbor if the merchant is compliant with PCI-DSS.49 In 2007, Minnesota enacted a payment card security law, which does not specifically reference PCI-DSS, but prohibits the retention of cardholder data, which is a core PCI-DSS requirement.50

---


50 Minn. Stat. § 325E.64 (2014).
Further, Massachusetts and California have adopted laws requiring security measures to protect personal information about their residents, which are broad enough to include payment card details. Massachusetts regulations require certain security controls for protecting the personal information of Massachusetts residents, including a written information security plan, risk assessments, vendor oversight, and certain specific security controls with administrative, technical and physical safeguards.51 California law does not include specific security controls, but does require that any business that collects personal information about California residents implement reasonable security measures and practices to protect that personal information.52 While states continue to pass laws and regulations requiring that personal information be protected, security programs consistent with PCI-DSS or other industry standards are likely to comply with current and future legislative requirements.

c. State Laws on Consumer Protection and Marketing

Most states have implemented consumer protection laws similar to the FTC's Section 5 prohibition against unfair and deceptive trade practices. These laws provide state regulators with powers to bring enforcement actions against businesses who use or share personal information in a manner inconsistent with privacy disclosures or unfair to consumers. While providing independent compliance requirements, these laws also are used as the enforcement mechanism for other privacy and security laws that do not contain their own enforcement provisions. For example, California Attorney General Kamala Harris recently used California's consumer protection law to bring an enforcement action against Kaiser Foundation Hospital for failing to notify residents affected by a data breach in a timely manner.53

California has further implemented statutes that require businesses to disclose how they share personal information collected on their websites with third parties for marketing purposes and how consumers are tracked through websites. California's “Shine the Light Law” requires businesses that disclose personal information to third parties for the third parties' own marketing purposes to provide certain details on these disclosures to consumers upon request.54 In addition, California requires that businesses make certain disclosures about information they collect on their websites and mobile Apps, including how they react to “Do Not Track” signals and whether third parties track consumers through the website and other third party websites.55 California regulators have released guidance on applying these requirements to mobile Apps.56

Some states bar merchants from requesting or requiring collection of personal information in a credit card transaction, unless certain conditions are met.57 Among the types

51 See 201 Mass Code Regs. 17.00.
53 Complaint for Injunction, Civil Penalties and Other Equitable Relief for Violations of Business and Professions Code Section 17200 (Unfair Competition Law), California v. Kaiser Foundation Health Plan, Inc., No. RG14711370 (Sup. Ct., Alameda County, filed and stipulation and final judgment entered Feb. 10, 2014).
56 See Kamala D. Harris, Attorney General, California Department of Justice, Privacy on the Go: Recommendation for the Mobile Ecosystem, (January 2013), http://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/privacy_on_the_go.pdf.
57 See, e.g., Cal. Civ. Code Sec. 1747 et seq.; MGL Ch. 93, Section 105(a) (Massachusetts).
of personal information to be restricted under the California law are zip codes and email addresses. These restrictions need to be considered by mobile payment providers as merchants may require certain information such as zip codes and email address to process customer transactions.

IV. FRANCHISING ISSUES IN MOBILE PAYMENT

Franchisors, like other retailers and service providers worldwide, are increasingly utilizing mobile payments options in connection with their businesses. Despite the potential additional complications of adopting a Mobile Payment Platform in a franchise system, there are a number of reasons that franchisors may want to consider mobile payments.

A. Key Drivers in Franchising

The general benefits of a mobile payments strategy, including customer convenience, data acquisition, targeted marketing, improved loyalty programs, cost reduction, and sales increases, are discussed above in Section II.E. However, there are two key strategic considerations that drive implementation of a Mobile Payment Platform in a franchise system.

1. Access to Customer Data

Traditionally, franchisors have had a limited ability to obtain information regarding the customers that patronize their franchise outlets. Many franchisors include provisions in their franchise agreement providing that all customer information collected by franchisees is owned by franchisor, that franchisor has the right to access customer information collected by franchisee, or that franchisees must provide customer information to franchisor upon termination. More recently, the implementation of system-wide loyalty and rewards programs have given franchisors more information. However, as discussed in Section II.E above, Mobile Payment Platforms significantly increase a franchisor’s ability to collect demographic information, purchasing preferences, marketing preferences, and contact information directly from the customers themselves.

2. Access to Revenue Stream

Another significant benefit to establishing a Mobile Payment Platform in a franchise system is increasing the franchisor’s ability to access information about the franchisee’s revenue stream. Typically, franchisors have to rely on franchisee reports or POS data to track franchisee sales. Similarly, franchisors have been limited to checks or ACH transfers to collect royalties from its franchisees. Mobile payments can provide increased transparency regarding franchisee revenue and accounting. For example, if the franchisor collects the payments made by customers using the Mobile Payment Platform, the adoption of a Mobile Payment Platform gives the franchisor unprecedented access to information regarding a franchisee’s revenue stream. Depending on the terms of the franchise agreement, the franchisor may even be able to deduct royalties or other payments due to franchisor directly from the revenue paid by the customers through a Mobile Payment Platform, rather than waiting for weekly or monthly payment from the franchisee.

B. Key Challenges in Franchising

1. Vicarious Liability

Because a Mobile Payment Platform is typically mandated by the franchisor, it is likely the franchisor will potentially be liable for any claims arising from the use of the Mobile Payment Platform. Under either an “instrumentality of the harm” test or “right to control” test, franchisors that specify POS or mobile payment systems may face liability. For example, since the passage of the FACTA in 2003, which created liability for retail locations that printed too much credit card information on receipt, franchisors have faced potential claims from franchisee customers. In *Keith v. Back Yard Burgers of Nebraska, Inc.*, a customer of a franchised location sued the franchisee and franchisor, claiming that there was too much information on the printed receipt that it received. Because the franchisor mandated the POS system that its franchisees used, the case was allowed to proceed. Similarly, in *Patterson v. Denny’s Corp.*, a court allowed a FACTA claim to proceed because the franchisor reserved the right to control operation of the location. For liability arising from Mobile Payment Platforms, the arguments are possible to be analogous. If a franchisor mandates the use of a Mobile Payment Platform, and a customer is harmed by its use of that platform, franchisor liability is likely. This is not necessary a reason to avoid mobile payments. Currently, the end-to-end encryption of mobile payments provides more protection for franchisees and the franchisor than the traditional system. However, the franchisor is still likely to be sued in the event of some violation linked to a franchisor’s system-wide Mobile Payment Platform.

2. Pricing

Most franchise systems allow franchisees some flexibility in setting prices for their products and services. Variations in pricing across a franchise system can create challenges for a Mobile Payment Platform. Either products and services must be tied to the location providing them, or franchisees must agree to comply with national pricing.

3. Adoption Issues

The success or failure of a mobile payment system as a marketing tool in a franchise setting depends in part on the consistency of experience of the customer using the system. Is it available at all locations? If it includes order-ahead capabilities, does it improve accuracy and speed of orders consistently? To ensure that a franchise system gets the most benefit from adopting a mobile payment system, it is imperative that franchisors achieve a high adoption rate by franchisees. Factors that affect the adoption rates of new technology include (a) the language in the franchise agreement, (b) the required investment in the new technology, and (c) the perceived benefit of the new technology.

   a. Franchise Agreements

While traditional non-franchised chains may find it relatively easily to ensure that the same mobile payment experience is available at all locations, franchisees are independent business owners operating under separate franchise agreements. Depending on the length of a


A franchisor’s ability to demand the adoption of mobile payments by existing franchisees depends on the terms of the franchise agreement. Franchise agreements and case law typically allow a franchisor to make changes to the franchise agreement at the end of a term when a franchisee is seeking to renew its agreement. However, the ideal introduction of a mobile payment system involves all locations at once, not just locations that have opted-in to a mobile payment system, or locations that are required to adopt a mobile payment system as a requirement for renewal. Many franchisors have franchise agreements that effectively allow a franchisor to impose reasonable new requirements on its franchisees by (a) requiring the franchisees to comply with the operations manual, and (b) providing that the operations manual and the system can be modified to keep up with changes in technology or economic realities. In addition, many franchise agreements expressly allow franchisors to dictate the POS hardware that is used in the business, or to require that franchisees participate in loyalty programs established by the franchisor. These provisions generally provide a sufficient basis for requiring that franchisees adopt a Mobile Payment Platform.

However, franchisees are often resistant to new technology and other system modifications, particularly if there are high costs involved. Occasionally, when a franchisor’s changes are seen as unreasonable, franchisees have been successful bringing claims based on the breach of an implied covenant of good faith and fair dealing. To avoid creating an unnecessarily adversarial relationship with franchisees, it is important for franchisors to explain the benefits and get franchisee buy-in prior to requiring a large franchise investment in a Mobile Payment Platform.

b. **Cost**

Adopting a mobile payment system can impose significant costs on a franchise system. There will be initial costs associated with the development of a Mobile Payment Platform, and additional costs associated with adoption of the system. Typically, adoption of mobile payment systems will involve at minimum (a) purchase and installation of additional hardware and software associated with the new technology, and (b) investments in training. Depending on the type of business and the current technology used in the system, costs can be a significant challenge. Even if the franchise agreement technically permits it, a franchisor must carefully consider whether it is reasonable to impose all of the changes that may be required of franchisees in order to implement a Mobile Payment Platform. It may be difficult for a franchisor to implement a mobile payment program, if its franchisees are not already using the same technology. In service based businesses, older systems, and international systems, franchisees may be less likely to have a standard POS system. Franchisees may be permitted to use personal computers of their own choice in connection with the business, or simply to self-report their sales. In addition, franchisees that operate outlets in non-traditional venues such as

---

61 See, e.g., Amos v. Union Oil Company of California, 663 F.Supp. 1027 (D.Ore. 1987) (holding that a gasoline franchisor’s modification of its system breached the implied covenant of good faith and fair dealing).

62 Bonfield v. AAMCO Transmissions, Inc., CCH ¶9469, 708 F.Supp. 867 (N.D. Ill. 1989) (noting that under Illinois law, even if a franchisor has a contractual right to change its policies, the implied duty of good faith requires the franchisor to make such changes reasonably and with proper motive).
stadiums, theme-parks, hotels, and airports, may be limited in their ability to change and/or implement new technology.

A franchisor’s right to impose new costs on its franchisees is also governed by the terms of the franchise agreement. Ideally, a franchisor which is planning to adopt a Mobile Payment Platform has a franchise agreement with a provision that allows the franchisor to modify the system to keep up with current technology, and expressly acknowledges that such changes may impose additional costs on franchisees. In the absence of such a provision, franchisees may be successful in refusing to comply with new technology requirements unless they are paid for by the franchisor. A franchisor should also consider if the adoption of a uniform system will provide enough benefits to the brand such that it would be appropriate for a national advertising fund to bear some or all of the cost. Most franchise systems have advertising fund language that is likely to be considered broad enough to cover the development costs of a mobile payment system. Alternatively, franchisors may give franchisees the option of using their required national or local advertising spending to help defray the additional costs imposed on franchisees by a new system. Such incentives can lead to higher participation rates.

c. Perceived Benefits

The most important part of getting a high rate of franchisee participation may be demonstrating significant benefits to franchisees. There are a number of potential ways to approach this. First, a Franchise Advisory Council (“FAC”) can be an invaluable part of determining whether to adopt a mobile payment system and to help evaluate what kind of system makes sense for the system. For example, when Dunn Bros. Coffee moved away from its plastic card loyalty program at the request of its franchisees, it relied on its Franchisee Marketing Council to evaluate the system that was to replace it. Similarly, Taco Bell and Dairy Queen have reported heavy franchisee involvement in the development of their Mobile Payment Platforms. Involving a FAC early in the process has multiple benefits. It gives the franchisor immediate feedback on the likely reaction of franchisees to the rollout of a mobile payment program, it creates ambassadors for the program, and it may generate volunteers for potential pilot test sites. Second, a successful pilot program can also be incredibly useful to ensuring franchisee buy-in. If a franchisor can demonstrate a good value proposition to franchisees, adoption rates will be high. For example, if the initial investment costs for franchisees will be relatively small, and the franchisor is able to present pilot program data to existing franchisees demonstrating increased customer loyalty, larger sales, more sales, and more opportunities for targeted marketing and promotion, then franchisees will be more likely to buy into the program.


64 See, e.g. Professional Shredding of Wisconsin, Inc. v. Proshred Franchising Corp., CCH ¶15,423, (S.D.N.Y., Sept. 5, 2013) (franchisor did not breach the franchise agreement by failing to use the advertising fund to create a national sales program – “the agreement endorses no particular use of the advertising fund, leaving to ProShred itself what use is ‘necessary or appropriate.’”); Burger King Corp. v. Hinton, CCH ¶12,329 (S.D. Fl., May 7, 2002) (noting that the franchise agreement provides allocation of advertising contributions at the discretion of Burger King’s business judgment); Burger King Corp. v. Agad, 941 F. Supp. 1217, 1222 (N.D. Ga. 1996) (no breach of contract for a donation to the Red Cross where franchise agreement provided that all advertising expenditures would be at BKC’s discretion).

V. BEST PRACTICES

Because Mobile Payment Platforms are an emerging technology, there is no one right way to develop and implement a mobile payment system. However, it is important to implement the kind of Mobile Payment Platform that addresses the specific needs of the particular franchise system. Below, the authors have identified the key stages of developing and implementing a Mobile Payment Platform as well as the key factors that should be considered at each stage.

A. Define Goals and Scope

☐ Convenience?
☐ Security?
☐ Increasing brand loyalty?
☐ Transition of loyalty/reward program?
☐ Cost savings?
☐ International? Domestic? Regional?
☐ Budget for project?

B. Solicit Franchisee Feedback and Involvement

☐ What are the franchisee needs?
☐ What are the franchisee benefits?
☐ Engage FAC to analyze and advocate.

C. Select Best Mobile Payment Platform For the System

☐ Consider franchisor and franchisee goals
☐ Review franchise agreements to assess implementation limitations
☐ Consider customer characteristics and desired brand experience
☐ Consider cost of development
☐ Consider cost of implementation

D. Identify Needed Vendor(s)

☐ Determine services needed (App Developer? Payment Processor? Hosting Services? Analytics?)
Consider vendor’s experience in relevant markets
Consider vendor’s experience with relevant mobile platforms
Consider vendor’s ability to deliver an experience consistent with brand and goals
Consider vendor’s reporting and analytics capabilities
Consider vendor’s ability to indemnify franchisor and franchisees

E. **Negotiate Necessary Agreements with Vendors and Franchisees**

- Determine control and ownership of IP
- Determine control and ownership of customer data
- Determine control obligations for legal compliance
- Clarify rights and obligations regarding direct marketing to customers
- Detail indemnification requirements
- Clarify support and training obligations
- Reporting and analytics requirements
- Discuss rebates
- Discuss brand support from vendors

F. **Assess Compliance/Legal Issues**

- Review financial, consumer protection, industry and other requirements
- Develop system to ensure compliance with franchisor obligations
- Understand rights and responsibilities regarding data protection and privacy
- Review and revise internal and external privacy policies
- Ensure franchisee compliance with reasonable data protection measures

G. **Develop Pilot Program**

- Identify representative test group (corporate/franchise, geographic diversity, diverse market size)
☐ Test, test, and test again
☐ Verify functionality across markets, store types, locations
☐ Assess user experience for convenience and brand consistency

H. Rollout System-wide
☐ Incorporate lessons learned from pilot program
☐ Determine and communicate value proposition for franchisees
☐ Market and promote

VI. CONCLUSION

Mobile payments currently represent a small portion of retail transactions, but the share of the market is growing. Mobile Payments Platforms represent a great opportunity for franchise systems, but there is a complicated web of legal and practical considerations, which are still developing, that franchisors and franchisees need to understand to determine the best approach for their system. If the growth in mobile payments continues, failing to offer mobile payment options may become a detriment to the brand, and many franchise systems may decide to jump in even if all the questions aren't answered. Franchise systems should continue to monitor the market and evaluate the best options for their system.
**Carol Anne Been** is an intellectual property lawyer at the international law firm, Dentons, working in the trademark, copyright, advertising and technology areas. She serves on the leadership team and is past chair of the Intellectual Property and Technology group for the US practice at Dentons. She was recognized as the 2015 "Lawyer of the Year" for Trademark Law in Chicago by The Best Lawyers in America. Carol Anne’s practice includes creating brand recognition and value through trademark clearance, prosecution, transactions and policing; development of ecommerce platforms and online delivery of products and services; licensing and merchandising programs; sweepstakes, contests and other advertising issues; managing privacy in marketing programs; and counseling on intellectual property strategy, structure, valuation, protection, management and enforcement. Carol Anne also is a panelist deciding domain name cybersquatting disputes under the Uniform Domain Name Dispute Resolution Policy (UDRP).

**Brian Carroll** is General Counsel at LevelUp, which provides a mobile-payments and customer rewards platform powering mobile apps for innovative retail brands throughout the country, as well as LevelUp’s own mobile app. Prior to joining LevelUp in January 2014, Brian was a partner with Foley Hoag, LLP in Boston, representing high-tech clients of all sizes in technology disputes and licensing. Brian earned a B.S. from Boston College in Computer Science and Finance, and also graduated from Boston College Law School.

**Keri McWilliams** is a franchise attorney with Nixon Peabody LLP in Washington, D.C. Keri works with franchisors to prepare and update franchise agreements and franchise disclosure documents in compliance with state, federal, and international franchise laws. She regularly counsels franchisors on sales compliance, franchisor/franchisee relationships, and international expansion. As a litigator, she has handled a wide range of commercial cases. In 2014 and 2015, Keri was recognized by Washington DC Super Lawyers as a "Rising Star" in the area of franchise and dealership. Keri received her J.D. from the Georgetown University Law Center and her B.F.A. from Washington University.