Mobile Payments Transactions and Contractual Considerations

May 27, 2015, 1:00PM – 2:00PM EDT

Speakers: Grace Powers, Bank of America, N.A.
Stephanie Sharron, Morrison & Foerster LLP
Judy Mok, Morrison & Foerster LLP
Chris Ford, Morrison & Foerster LLP

1. Presentation

2. 2013 OCC Guidance on Third Party Service Providers” as published in the American Bar Association Consumer Financial Services Committee Newsletter dated 2/25/15 by Joan Warrington and Judy Mok

3. Mobile Payments Legal Issues: A Primer
Mobile Payments Transactions and Contractual Considerations

May 27, 2015

Presented By

Stephanie Sharron, Grace Powers, Judy Mok, Chris Ford
Overview

• Current Landscape and Emerging Technologies
• Consumer Considerations and related Regulations
• Considerations for Financial Institutions when Contracting with Service Providers
• Data Usage
What are Mobile Payments?

Broadly, “mobile payments” are payment transactions made using a mobile device and payment instruments such as cash, bank accounts, debit/credit cards or stored value accounts (e.g., transit cards, gift cards, PayPal, or mobile wallets).
The Mobile Payments Ecosystem: It’s Complex!

- Banks and card issuers
- Mobile operators
- Retailers
- Device suppliers
- Service providers
- Trusted Service Managers
Some Key Players in Mobile Payments
Mobile Payments Methods Overview

- Payment Methods/Approaches
  - Digital Wallets (e.g., PayPal, GooglePay)
  - Contactless Cards and traditional credit cards (e.g., Visa, MasterCard)
  - QR Codes (e.g., CurrentC)
  - Bar Codes (e.g., Starbucks)
  - SMS/USSD (e.g., Boku, M-Pesa)
  - Mobile Device as Point-of-Sale (e.g., Square)
  - P2P (e.g., Venmo)
  - FiSync (e.g., Dwolla)
  - Point-of-Sale Terminal (e.g., Verifone)

- Key Underlying Technologies
  - Encryption (e.g., point-of-sale systems)
  - Tokenization: HCE (e.g., Visa, MasterCard, AmEx), Secure Element (ApplePay) and others
<table>
<thead>
<tr>
<th>Player Name</th>
<th>Offering Description</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Wallet</td>
<td>Digital Wallet, Consumer Payment Solution</td>
<td>Mobile Device NFC Tokenization</td>
</tr>
<tr>
<td>Apple Pay</td>
<td>Digital Wallet, Consumer Payment Solution</td>
<td>Mobile Device NFC Secure Element Tokenization Biometric: Touch ID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Network-level Tokenization</td>
</tr>
<tr>
<td>Stripe</td>
<td>Stripe Connect, Stripe Checkout</td>
<td>API and developer toolkit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Embeddable payment form (desktop or mobile)</td>
</tr>
<tr>
<td>PayPal</td>
<td>Digital Wallet, PayPal Here</td>
<td>Browser, iOS, and Android apps</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mobile device card reader attachment</td>
</tr>
<tr>
<td>Visa</td>
<td>Visa Network, payWave, Visa Digital Solutions</td>
<td>EMV./HCE Tokenization</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RFID chip embedded into smart cards</td>
</tr>
<tr>
<td></td>
<td></td>
<td>API and developer toolkit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mPOS</td>
</tr>
<tr>
<td>Player Name</td>
<td>Offering Description</td>
<td>Technology</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Samsung LoopPay</td>
<td>mPOS hardware solution</td>
<td>Mobile device card reader attachment</td>
</tr>
<tr>
<td>Alipay</td>
<td>Digital wallet, Alipay ePass</td>
<td>Browser, iOS, and Android apps Facial recognition</td>
</tr>
<tr>
<td>Amazon Payments</td>
<td>Digital wallet, Amazon PayPhrase</td>
<td>mPOS software Browser software</td>
</tr>
<tr>
<td>Verifone</td>
<td>PoS terminals</td>
<td>NFC, contactless smart cards, swipe-card</td>
</tr>
<tr>
<td>LevelUp</td>
<td>Digital wallet, analytics</td>
<td>iOS and Android app</td>
</tr>
<tr>
<td>Venmo (Braintree)</td>
<td>P2P money transfer</td>
<td>Cardholder tokenization system, iOS and Android app</td>
</tr>
<tr>
<td>Dwolla</td>
<td>Digital wallet, P2P money transfer</td>
<td>Tokenization, API and developer toolkits Browser, iOS, and Android apps</td>
</tr>
<tr>
<td>MCX/CurrentC</td>
<td>Digital wallet</td>
<td>QR Codes, iOS and Android app</td>
</tr>
<tr>
<td>Boku</td>
<td>P2P money transfer</td>
<td>SMS, mobile carrier billing</td>
</tr>
</tbody>
</table>
What is Encryption?

• Encryption is the process by which plain-text data is transformed into non-readable form using an algorithmic process.
  • Session-level encryption: here it is helpful to think of the data as being stored in a pipe, and the protection occurring in the wall of the pipe but not at the data level itself.
  • Data encryption: here the data itself (sometimes referred to as the “payload”) is transformed, so that wherever that data resides and whomever accesses it cannot obtain the sensitive information without decrypting the data.
• Decryption requires a key (also an algorithm).
• Encryption can use symmetric keys or asymmetric keys (e.g., as in public-private key cryptography, or PKI)
What is Tokenization

• Tokenization is the process of substituting a sensitive data element, such as the primary account number (PAN), with a non-sensitive surrogate value that is randomly generated, so that the sensitive data element cannot be derived from the surrogate value alone.

• Tokenization differs from encryption in that the token is a random string of numbers and not algorithmically derived.
How are encryption and tokenization be used in payment transactions?

- Either or both session-level and data encryption can be used to secure the primary account number of a credit or debit card when collected at the point-of-sale prior to authorization of the payment.
- Encryption can also be used to secure the data when transmitted to the payment processor.
- Tokenization can be used after payment authorization to avoid storage and transmission of the primary account number. Instead, a “token” is used to substitute for the sensitive PAN.
- In tokenization, encryption also is used to secure the PAN and other sensitive data in the token vault. Often this function is served by a third party token service provider.
Tokenization Roles

• **Token Requestors**
  • Any party that registers with a Token Service Provider and requests tokenization services
  • Could be potentially anyone in the transaction stream, including merchants, acquirers, payment enablers, digital wallet providers, or card issuers

• **Token Service Providers**
  • Provide payment tokens to registered Token Requestors, manage the token vault, and responsible for security and controls around the provisioning of tokens
  • Could be an issuer, a merchant, or a payment network
EMV and the EMV Specification

• EMVCo is an organization created to facilitate worldwide interoperability with and acceptance of the EMV Specification.

• EMV is a global standard for inter-operation of integrated circuit cards (IC cards or "chip cards") and IC card capable point of sale (POS) terminals and automated teller machines (ATMs), for authenticating credit and debit card transactions

• EMV provides protection for both card present transactions and card-not-present transactions, and adopts a tokenization approach to address security and reduce fraud
Payment Token Transaction Overview
EMV Token Provisioning

Figure 1: Payment Token Provisioning Overview
Underlying Technology for EMV: Host Card Emulation (HCE)

- **Host Card Emulation (HCE)**
  Permits an NFC-enabled mobile device to perform card emulation without relying on access to a secure element (SE)
  - Payment credentials are stored on secure cloud databases
  - Trusted mobile app manages card emulation function and verification by communicating through an application management platform to the credit card network to complete transactions
  - Mobile device is in constant contact with backend systems to receive updates, test information, and provide data to respond to risk tolerance of issuers
  - Relies on the EMV (Europay, Mastercard, Visa) specification
Underlying Technology: HCE

NFC Reader

Mobile Device

NFC Controller

CPU

Secure Cloud
Underlying Technology: HCE
Underlying Technology: HCE
Underlying Technology: HCE
Underlying Technology: HCE
Apple Pay

- **Apple Pay** is a digital wallet and mobile payment platform compatible with newer iOS devices.
- **Secure Element (SE)**
  Tamper-resistant platform that stores payment credentials on the device and securely executes applications, processes cryptographic data, and communicates with external NFC readers.
- **Apple Touch ID**
  Fingerprint reader built into the iPhone and other devices.
- **Apple Pay tokenization uses Secure Element**
  Instead of storing credit card credentials, Apple Pay stores a token in its SE generated by partner credit card networks.
Underlying Technology: SE

NFC Reader
Underlying Technology: SE

NFC Reader

Mobile Device

NFC Controller

Secure Element

CPU
Underlying Technology: SE

NFC Reader

Mobile Device

NFC Controller

Secure Element

CPU
Emerging Commercial Issues

• Security concerns can spook consumers
  • HCE is being rolled out and endorsed by MasterCard and Visa, but some ecosystem players may not have sufficient network-based security measures
  • Apple TouchID, a biometric fingerprint scanner and a key security feature of Apple Pay, was hacked by security researchers through “brute-forcing”

• Key impediment for retailers: cost of PoS terminals
  • Many retailers are hesitant to install compatible machines

• Too many wallets can overwhelm consumers
  • Retailers, banks, restaurants, credit cards and mobile networks are each releasing apps that operate as wallets or payment methods

• Regulatory Hurdles
  • Differing consumer protections depending on the payment sources (e.g., credit card, prepaid card, mobile carrier billing)
  • Privacy concerns
Consumer’s Use of Mobile Payments

• How do consumers initiate a mobile payment? Using a mobile phone, mobile app, mobile web or SMS text message.

• What kind of mobile payments are consumers making? Federal Reserve Board Report on Consumer and Mobile Financial Services (March 2015) looked at the trends in the last 12 months:
  • 68% paid bills
  • 54% made online or in-app purchases
  • 39% paid for a product or service in store
  • 36% made a person to person transfer within the U.S.
  • 31% received money from another person using a mobile device
  • 30% received loyalty or reward points
  • 16% paid for parking, taxi or public transit
  • 11% made a text message payment
  • 9% made an international remittance transfer
Consumer Considerations for Mobile Payment Solutions

- How can I easily make a payment?
- Can I make it quickly?
- How is the payment funded?
  - Deposit accounts, debit or credit cards
  - Prepaid, stored value or gift card
  - Nonbank accounts (e.g., Paypal)
  - Mobile phone carrier bill
- What do I do if there’s a problem?
  - Reporting fraud, disputes or errors
  - Liability for losses
- Who is seeing my information?
## Mobile Payments Regulation

### What may apply?
- eSign
- Regulation E (EFTA)
- Regulation Z (TILA)
- Regulation P (GLBA)
- FCRA
- FFIEC – Authentication Guide
- UDAAP
- TCPA
- State money transmitter laws
- Bank Secrecy Act
- Anti-money laundering

### Who are the regulators?
- CFPB
- OCC
- FFIEC
- FTC
- FinCEN
- States
  - State financial institution or money transmitter regulators
  - State attorneys general
Contracting with Consumers

- Electronic Signatures in Global and National Commerce Act (E-Sign) – For laws or regulations that require consumer disclosures to be “in writing”:
  - Agreement to electronic disclosures instead of paper
  - E-Sign consent disclosures – Informs consumers of the option to receive disclosures in paper form, the right to withdraw consent, how to obtain paper copies, and the hardware/software requirements for access and retention.
  - Affirmative consent must be obtained electronically in a manner that reasonably demonstrates that the consumer will be able to access required notices or disclosures electronically.
- ESIGN does not trump legal requirements concerning content, formatting (font size, presentation), timing of delivery, or verification or acknowledgment or receipt with respect the disclosures being electronically delivered.
- For disclosures that are required to be in writing, ESIGN does not consider oral disclosures to be a valid form of electronic delivery.
- Use of electronic signatures – Click signatures, digitized handwritten signatures, and biometrics.
Regulation E (Electronic Funds Transfers)

- Applicable to payments funded from consumer asset accounts (e.g., checking, savings) and done via debit card, online, mobile or other access devices.

- **Initial Disclosures:** Must be given at the time the consumer contracts for an EFT service or before the first EFT has been made. 12 CFR § 1005.7(b). See Appendix A, Model Form A-2 for sample clauses.
  - Disclosures discuss consumer liability for unauthorized electronic fund transfers, types of transfers allowed and limitations, fees, liability of financial institution for failure to make or stop transfers and error resolution.

- **Error Resolution Disclosure:** Must be mailed or delivered once per calendar year. 12 CFR §§1005.7(b)(10) and 1005.8(b). See Model Form A-3 for sample clauses.
Regulation E – Remittance Transfers

• Applicable to electronic funds transfers requested by a US consumer to a recipient in a foreign country and sent by a remittance transfer provider
  • Can cover banks and nonbanks.

• **Prepayment disclosure:** Must include transfer amount sent (in funding currency), transfer fees and taxes, total sent, exchange rate used, the transfer amount received in the recipient’s currency, and other transfer fees.

• **Receipt:** Must include date on which funds will be available to recipient, recipient contact information, error resolution and cancellation rights, remittance transfer provider contact information (name, telephone number, and website).

• Disclosures can be written or oral, sent through a mobile app or text messages. If sent via mobile app or text message, disclosures do not need to be in retainable form.
Regulation Z (Truth in Lending)

- Applicable to mobile payments where the payment is funded through consumer credit.

- **Account Opening:** 12 CFR § 1026.6(b)(2) requires account-opening disclosures for open-end credit, such as APR, introductory rates, fees, charges.
  - Certain disclosures must be in tabular format with headings, content and format substantially similar to the applicable tables in G-17.
  - Other disclosures, such as billing error rights, when charges may be imposed, balance computation method, variable rates, initial rates, need to be provided as well (typically contained in credit card agreement).
  - Creditor must post or maintain cardholder’s credit card agreement on its website or provide a copy upon request.

- **Liability for Unauthorized Use:** 12 CFR § 1026.12(b)(2) – A cardholder shall be liable for unauthorized use of a credit card only if it’s an accepted credit card, issuer has provided means to ID the cardholder, and adequate notice is provided regarding max liability ($50 or lesser amount) and the means by which issuer can be notified of loss or theft of card;
• **Regulation P**, which implements the Gramm-Leach Bliley Act, requires initial and annual notices to customers that adequately reflect the financial institutions privacy policies and practices.

• **California Online Privacy Protection Act (“CalOPPA”)** – Requires operators of websites or online services that collect personal information to clearly and conspicuously post its privacy policy and comply with that privacy policy.

• **Children’s Online Privacy Protection Act** – Must post a clear and comprehensive privacy policy describing information practices for personal information collected online from children under 13.
Tips for Consumer Agreements

• Design challenges in the mobile space for smaller screens and non-standard ways of keeping copies of disclosures

**G-17(B) Account-Opening Sample**

<table>
<thead>
<tr>
<th>Interest Rates and Interest Charges</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Annual Percentage Rate (APR) for Purchases</strong></td>
<td><strong>8.99%</strong></td>
</tr>
<tr>
<td></td>
<td>This APR will vary with the market based on the Prime Rate.</td>
</tr>
<tr>
<td><strong>APR for Balance Transfers</strong></td>
<td><strong>15.99%</strong></td>
</tr>
<tr>
<td></td>
<td>This APR will vary with the market based on the Prime Rate.</td>
</tr>
<tr>
<td><strong>APR for Cash Advances</strong></td>
<td><strong>21.99%</strong></td>
</tr>
<tr>
<td></td>
<td>This APR will vary with the market based on the Prime Rate.</td>
</tr>
<tr>
<td><strong>Penalty APR and When it Applies</strong></td>
<td><strong>28.99%</strong></td>
</tr>
<tr>
<td></td>
<td>This APR may be applied to your account if you:</td>
</tr>
<tr>
<td></td>
<td>1) Make a late payment;</td>
</tr>
<tr>
<td></td>
<td>2) Go over your credit limit twice in a six-month period;</td>
</tr>
<tr>
<td></td>
<td>3) Make a payment that is returned; or</td>
</tr>
<tr>
<td></td>
<td>4) Do any of the above on another account that you have with us.</td>
</tr>
<tr>
<td><strong>How Long Will the Penalty APR Apply?</strong></td>
<td>If your APRs are increased for any of these reasons, the Penalty APR will apply until you make six consecutive minimum payments when due.</td>
</tr>
<tr>
<td><strong>Paying Interest</strong></td>
<td>Your due date is at least 25 days after the close of each billing cycle. We will not charge you any interest on purchases if you pay your entire balance by the due date each month. We will begin charging interest on cash advances and balance transfers on the transaction date.</td>
</tr>
<tr>
<td><strong>Minimum Interest Charge</strong></td>
<td>If you are charged interest, the charge will be no less than $1.50.</td>
</tr>
<tr>
<td><strong>For Credit Card Tips from the Consumer Financial Protection Bureau</strong></td>
<td>To learn more about factors to consider when applying for or using a credit card, visit the website of the Consumer Financial Protection Bureau at <a href="http://www.consumerfinance.gov/learnmore">http://www.consumerfinance.gov/learnmore</a></td>
</tr>
</tbody>
</table>

**Fees**

| Annual Fee | None |
| Transaction Fees | Balance Transfer |
| | Either $5 or 3% of the amount of each transfer, whichever is greater (maximum fee: $100). |
Tips for Consumer Agreements

- See FTC Dot Com Disclosure Guide 2.0 for ideas on how to make things clear and conspicuous, and potentially reduce the risk of UDAP (UDAAP for CFPB) issues.
  - Scrolling is not favored, unless you can use text or visual cues to inform customers to scroll for viewing the entire disclosure.
  - Must design disclosures to account for viewing on different devices.
  - Hyperlinks are discouraged, but if necessary:
    - Use clear labeling
    - Place link near qualified claim
    - Take consumers directly to disclosures
  - Monitor click through rates
Tips for Consumer Agreements

• Use email to send out the disclosures and agreements that customer saw and agreed to during the mobile session and transaction confirmations.
  • Provide tips to mobile users on how they can print or save disclosures on different devices.

• Require explicit consent (such as a click through or check box) before customer can use mobile payment service.

• Use just-in-time disclosures or notifications.
Considerations for Financial Institutions ("FIs") When Contracting with Mobile Payments Service Providers

- Mobile payments present same types of risks to FIs associated with many traditional banking-related products, e.g., fraud, reputation, and vendor management.
- FIs may not have the same level of control over mobile payments interactions as they would over traditional bank products as FIs may not be in privity with all the mobile payments participants.
- Mobile payments require the coordinated and secure exchange of payment information among several unrelated entities.
Importance of Vendor Management in Mobile Payments

• Mobile payments third-party providers may not be knowledgeable about the regulatory environment in which FIs operate.
• Effective management of risks may involve FIs partnering with application developers, mobile network operators, handset manufacturers, specialized security firms, and other third party service providers.
• FIs are expected to be prudent in choosing appropriate third party service providers in mobile payments transactions and monitoring the performance of these providers, beginning with contract negotiations with these companies.
“Critical activities” = significant bank functions (e.g., payments, clearing, settlements, custody) or significant shared services (e.g., information technology), or other activities that:

- (i) could cause a bank to face significant risk if the third party fails to meet expectations;
- (ii) could have significant customer impacts;
- (iii) require significant investment in resources to implement the third-party relationship and manage the risk; and
- (iv) could have a major impact on bank operations if the bank has to find an alternate third party or if the outsourced activity has to be brought in-house.

The OCC expects to see certain types of contractual provisions in banks’ agreements with their service providers, including mobile payments providers. (See Appendix 1)

❖ Some key topics mentioned in the OCC Guidance include:
  ➢ Responsibility for Compliance with Applicable Laws
  ➢ Indemnification
  ➢ Default and Termination
Examples of OCC Guidance and Practical Tips: Responsibility for Compliance with Applicable Laws and Regulations

OCC Guidance:

- Ensure bank has right to monitor on an ongoing basis third party’s compliance with applicable laws, regulations and policies and requires remediation if issues arise.

Practical Tips:

- When drafting contract, consider distinguishing between e.g., “Bank Applicable Law” vs “Mobile Payments Service Provider Applicable Law”.
- Delineate applicable laws that are unique to a party that would govern that party’s provision of services or activities under the agreement.
- A party should be responsible for instructing the other party to comply with its set of applicable laws if the two sets of applicable laws relate to different industries and are different in scope.
Examples of OCC Guidance and Practical Tips: Indemnification/Limits on Liability

**OCC Guidance:**

- Specify extent of bank liability for third party failure to perform, assess indemnification clauses that require bank to hold third party harmless from liability, and consider whether proposed limit is in proportion to the amount of loss bank might experience because of third party’s failure to perform or comply with applicable laws.

**Practical Tips:**

- Unlike most banking products that allow institutions to control much of the interaction, mobile payments require the coordinated and secure exchange of payment information among several unrelated entities. May have more success in negotiating with a party by asking such party to take on risks that are within its control.

- Which party is engaging in the activities that are more likely to incur liability?

- Which party has more consumer facing risk and liability? Are there risks of class action lawsuits?
Examples of OCC Guidance and Practical Tips: Termination Rights

OCC Guidance:

- Include “a provision that enables the bank to terminate the contract, upon reasonable notice and without penalty, in the event that the OCC formally directs the bank to terminate the relationship.”

Practical Tips:

- Negotiate termination rights for changes in applicable law.
- Define “applicable law” broadly to include not just statutes and regulations, but also regulatory guidance, orders and interpretations of governmental authorities.
- Exit rights if there are material adverse effect on either party or on the mobile payments program (e.g., reputational harm, litigation risks, change in law).
A balancing act in negotiations

- While the OCC Guidance identifies best practices, in reality, parties to a mobile payments transaction are involved in a commercial negotiation.
- Not surprisingly, FIs use the OCC Guidance as leverage to negotiate more bank favorable provisions in their contracts with mobile payments third party providers, in particular with respect to bank approval rights and oversight and control of these companies.
Practical Considerations:

- Market reality will dictate how the parties will negotiate based on:
  - Who are the parties?
  - Who does what?
  - Who pays for what?
  - What risks are within a party’s control? Who is in best position to bear the risks?
  - What laws apply to which parties?
  - What activities are being undertaken by each party?
APPENDIX 1: 2013 OCC Guidance provides that banks’ contracts with third party service providers should address the following topics:

1. Nature and Scope of Arrangement
2. Performance Measures or Benchmarks
3. Responsibilities for Providing, Receiving, and Retaining Information
4. The Right to Audit and Require Remediation
5. Responsibility for Compliance with Applicable Laws and Regulations
6. Cost and Compensation
7. Ownership and License
8. Confidentiality and Integrity
9. Business Resumption and Contingency Plans
10. Indemnification
11. Insurance
12. Dispute Resolution
13. Limits on Liability
14. Default and Termination
15. Customer Complaints
16. Subcontracting
17. Foreign-Based Third Parties
18. OCC Supervision
What is Transaction Data?

**TRANSACTION DATA** means information required by transaction participants to evidence Charges or Credits

- **USUALLY** Information obtained at the point of sale
- **NOT** information regarding object of transactions like products purchased or identity of custody
- **IS** reference data describing time, place, prices, payment methods, discount values, chargebacks and quantities
- **CAN INCLUDE** information obtained or generated during Authorization and settlement
- **DOES NOT INCLUDE** Cardholder Data

*Cardholder Data* is data on the magnetic stripe or the primary account number, and includes cardholder name, service code, and expiration date.
What is the nature of the Data?

• What constitutes Transactions Data is a moving target at best
• We know that data in the system morphs as it passes from transaction participant to transaction participant through the payment ecosystem
What is the nature of the Data?

- What constitutes Transactions Data is a moving target at best
- We know that data in the system morphs as it passes from transaction participant to transaction participant through the payment ecosystem
What is the nature of the Data?

- What constitutes Transactions Data is a moving target at best
- We know that data in the system morphs as it passes from transaction participant to transaction participant through the payment ecosystem

Payment System Facilitator (PayPal, Square, etc.)

Information of multiple Cardholders, Issuers and Merchants
What is the nature of the Data?

- What constitutes Transactions Data is a moving target at best
- We know that data in the system morphs as it passes from transaction participant to transaction participant through the payment ecosystem
What is the nature of the Data?

- What constitutes Transactions Data is a moving target at best
- We know that data in the system morphs as it passes from transaction participant to transaction participant through the payment ecosystem
What is the nature of the Data?

- What constitutes Transactions Data is a moving target at best
- We know that data in the system morphs as it passes from transaction participant to transaction participant through the payment ecosystem
What is the nature of the Data?

- What constitutes Transactions Data is a moving target at best
- We know that data in the system morphs as it passes from transaction participant to transaction participant through the payment ecosystem
What is the nature of the Data?

- What constitutes Transactions Data is a moving target at best
- We know that data in the system morphs as it passes from transaction participant to transaction participant through the payment ecosystem

- It is unclear who really owns the Transaction Data and may lay claim to it?
- Given the lack of clarity, how may the ecosystem participants use it?
What are the Interests in the Data?

According to Gartner, Big Data is “high volume, high velocity and/or high variety information assets” that can be used to improve decision making and provide better insights.

- **Transaction Data is “Big Data” in the payments ecosystem**

  At the end of the day, each participant in the ecosystem is either attempting to improve the experience for their customers or to monetize the information they are gathering

- **For Merchants, it’s all about the data analytics**
  - Understanding who their customers are
  - Predicting customers’ buying habits
  - Understanding ways to market to them to entice them to spend more on the retailer’s products and services
  - Identifying cost-cutting measures, product improvements and customer retention strategies

- **Issuers**
  - Identifying the **best** potential new cardholders
  - Retaining existing high-value cardholders by catering to their use habits
  - Devising communication strategies that address the needs of different customer segments
What are the Interests in the Data?

• Acquirers, Processors and Payment System Facilitators have the ability to aggregate data of many merchants
  • The ability to provide information to a merchant regarding its competitive position in the market
  • Providing information regarding trending in markets
  • Creating models for consumer shopping and consumer trends

• Payment Brands
  • Monetizing information gathered from spending trends of customers
  • Fraud Protection
  • Driving analytics to acquire and retain merchant use of applicable network
  • Acting as the traffic cop and setting the rules

• Mobile Providers
  • Monetizing information gathered about customers’ preferences and online interactions
  • Create technology offerings that distinguish them from competitors
Contractual and Data Sharing Relationships

• **Contracts are generally bi-lateral**
  • But many different contractual relationships touch the transaction
  • Upstream and downstream participants may place restrictions on use of data that must flow through them
Contractual and Data Sharing Relationships

- Contracts are generally bi-lateral
  - But many different contractual relationships touch the transaction
  - Upstream and downstream participants may place restrictions on use of data that must flow through them
Contractual and Data Sharing Relationships

- Contracts are generally bi-lateral
  - But many different contractual relationships touch the transaction
  - Upstream and downstream participants may place restrictions on use of data that must flow through them
Contractual and Data Sharing Relationships

- Contracts are generally bi-lateral
  - But many different contractual relationships touch the transaction
  - Upstream and downstream participants may place restrictions on use of data that must flow through them

Diagram:
- Merchant
- Payment System Facilitator
- Customer/Consumer
- Issuer
Contractual and Data Sharing Relationships

- Contracts are generally bi-lateral
  - But many different contractual relationships touch the transaction
  - Upstream and downstream participants may place restrictions on use of data that must flow through them

```
Merchant <-> Processor

Payment System Facilitator

Customer/Consumer <-> Issuer
```
Contractual and Data Sharing Relationships

- Contracts are generally bi-lateral
  - But many different contractual relationships touch the transaction
  - Upstream and downstream participants may place restrictions on use of data that must flow through them
Contractual and Data Sharing Relationships

- Contracts are generally bi-lateral
  - But many different contractual relationships touch the transaction
  - Upstream and downstream participants may place restrictions on use of data that must flow through them
Contracts are generally bi-lateral

- But many different contractual relationships touch the transaction
- Upstream and downstream participants may place restrictions on use of data that must flow through them
• **Contracts are generally bi-lateral**
  - But many different contractual relationships touch the transaction
  - Upstream and downstream participants may place restrictions on use of data that must flow through them
Contractual and Data Sharing Relationships

- **Contracts are generally bi-lateral**
  - But many different contractual relationships touch the transaction
  - Upstream and downstream participants may place restrictions on use of data that must flow through them
Contractual and Data Sharing Relationships

- Contracts are generally bi-lateral
  - But many different contractual relationships touch the transaction
  - Upstream and downstream participants may place restrictions on use of data that must flow through them
Data Ownership and Contractual Considerations

• Ownership of Transaction Data is an amorphous concept
  • Only thing for certain is Customers own their Personal Information and only grant other parties the right to use it
  • Multiple ecosystem participants have relationships with the customer (Issuer, Mobile Provider, Payment System Facilitator) which complicates rights and ownership
  • Issuers may have greatest claim to ownership of Transaction Data
    • Have the relationship with the customer
    • Authorize the transaction
  • Because the data is ever changing, better to consider rights of use vs. ownership

Card Brands are likely the greatest influencers on use rights since they are the closest to policing the ecosystem and the transactions
What Generally Goes into the Contract?

- Protection against claims from upstream or downstream transaction participants
  - Flow-down/mandatory provisions
  - Definition of allowable uses
  - Distinguishing between Customer Data and Cardholder Data
  - Indemnification against unauthorized use

- Protecting Identities
  - Aggregate, De-Identify and Anonymize Information for any allowable use
  - Market concentration can be a factor
  - Opt-ins and Opt-Outs
What Generally Goes into the Contract?

• Compliance with Laws, Rules and Policies
  • GLBA and other Federal and State Privacy Laws
  • Network Rules
  • PCI Compliance
  • Adherence to Privacy Policies

• Miscellaneous Considerations
  • Termination Rights
  • Post-Termination Responsibilities/Rights
  • Specific Enforcement Rights
Questions?

Stephanie Sharron  
Partner  
Palo Alto  
Technology Transactions Group  
ssharron@mofo.com  
(650) 813-4018

Chris Ford  
Partner  
Washington, D.C. Technology Transactions Group  
cford@mofo.com  
(202) 887-1512

Judy Man Ni Mok  
Associate  
New York Financial Services Group  
jmok@mofo.com  
(212) 336-4073

Guest Speaker:

Grace Powers  
Associate General Counsel, SVP  
Bank of America, N.A.  
grace.powers@bankofamerica.com  
(213) 345-8698
Grace Powers is Senior Vice President and Associate General Counsel with Bank of America. She is the lead lawyer providing support to Bank of America’s Consumer Banking digital product development group and is the Bank’s resident legal expert on the Electronic Signatures in Global and National Commerce Act (E-Sign) and the Uniform Electronic Transactions Act (UETA). Her experience includes advising on electronic signatures and transactions, electronic funds transfers, online privacy and data security, authentication, and website and mobile accessibility.

Grace is a frequent speaker on legal issues related to electronic commerce in consumer financial services and has contributed articles on the subject to numerous publications. In 2009, Grace was named a Technology All-Star by Mortgage Banking Magazine. She currently serves as Co-Chair of Publications and Membership Vice-Chair to the Consumer Financial Services Committee of the ABA Business Law Section. She is admitted to practice law in California, Oregon and Washington.

grace.powers@bankofamerica.com
(213) 345-8698
2013 OCC Guidance on Third Party Service Providers

By Joan Warrington and Judy Mok, Morrison & Foerster LLP

Third party service providers are an integral part of the financial services industry, providing critical functionalities (e.g., credit decisioning support, payment processing services, records retention, documents destruction) to financial institutions and other participants in the payment process. Given the complexity of services provided, financial institutions may face significant operational difficulties in transferring the services of such third party service providers that fail to meet appropriate service levels. Given the sensitive nature of information to which these third party service providers may have access, including personally identifiable information belonging to customers of financial institutions, regulators expect financial institutions to be accountable for the actions of the companies with which they contract. Financial institutions are expected to be prudent in choosing appropriate third party service providers and monitoring the performance of these providers, beginning with contract negotiations with these companies.

On October 30, 2013, the Office of the Comptroller of the Currency (“OCC”) issued a Risk Management Guidance on Third-Party Relationships1 (“2013 OCC Guidance”) which sets forth detailed expectations for national banks and federal savings associations with respect to assessing and managing risks associated with their relationships with third party service providers. The 2013 OCC Guidance calls for more comprehensive and rigorous oversight and management of third party relationships that involve “critical activities.” The 2013 OCC Guidance defines “critical activities” as significant bank functions (e.g., payments, clearing, settlements, custody) or significant shared services (e.g., information technology), or other activities that: (i) could cause a bank to face significant risk if the third party fails to meet expectations; (ii) could have significant customer impacts; (iii) require significant investment in resources to implement the third-party relationship and manage the risk; and (iv) could have a

major impact on bank operations if the bank has to find an alternate third party or if the
outsourced activity has to be brought in-house. Most notably, the 2013 OCC Guidance includes
the types of contractual provisions the OCC expects to see in banks’ agreements with their
service providers. According to the 2013 OCC Guidance, “developing a contract that clearly
defines expectations and responsibilities of the third party helps to ensure the contract’s
enforceability, limit the bank’s liability, and mitigate disputes about performance.” Specifically,
the 2013 OCC Guidance provides that banks’ contracts with third party service providers should
address the following topics:

1. Nature and Scope of Arrangement
2. Performance Measures or Benchmarks
3. Responsibilities for Providing, Receiving, and Retaining Information
4. The Right to Audit and Require Remediation
5. Responsibility for Compliance with Applicable Laws and Regulations
6. Cost and Compensation
7. Ownership and License
8. Confidentiality and Integrity
9. Business Resumption and Contingency Plans
10. Indemnification
11. Insurance
12. Dispute Resolution
13. Limits on Liability
14. Default and Termination
15. Customer Complaints
16. Subcontracting
17. Foreign-Based Third Parties
18. OCC Supervision

The 2013 OCC Guidance provides detailed descriptions of the issues that need to be
addressed with respect to each of the foregoing topics in the contracts between banks and their
third party service providers. For example, the 2013 OCC Guidance states that a contract should
include “a provision that enables the bank to terminate the contract, upon reasonable notice and
without penalty, in the event that the OCC formally directs the bank to terminate the
relationship” and also addresses limitation of liability, asking “whether the contract limits the
third party’s liability and whether the proposed limit is in proportion to the amount of loss the
bank might experience because of the third party’s failure to perform or to comply with
applicable laws.” It also “prohibits the third party and its subcontractors from using or disclosing
the bank’s information, except as necessary to provide the contracted activities or comply with
legal requirement.” Not surprisingly, many banks and other financial institutions use the 2013 OCC Guidance as leverage to negotiate more bank favorable provisions in their contracts with their service providers, in particular with respect to bank approval rights and oversight and control of their service providers. While some companies may feel that this gives banks unfair negotiating leverage, the key takeaway from the 2013 OCC Guidance and other regulatory guidance on this issue (as noted below) is that service providers will be held to the same standards to which the regulated entity is subject. Therefore, these standards provide flexibility depending on the risks the particular services pose to the financial institutions, their customers and operations. Even entities that are not under OCC supervision, but involved in third party service provider relationships, should consider using the 2013 OCC Guidance as a “best practices” guide. For banks and federal savings associations that are under the supervision of the OCC, it is crucial to review the 2013 OCC Guidance and make sure they manage their third party service provider relationships accordingly and meet the expectations of the 2013 OCC Guidance when negotiating contracts with their service providers.

As conveyed in the 2013 OCC Guidance, the OCC expects banks to practice effective risk management regardless of whether such banks perform the activity internally or through a third party. Similarly, other regulators have issued bulletins and guidance on their expectations with respect to how banks and other financial institutions should manage their relationships with third party service providers. For example, in April 2012, the Consumer Financial Protection Bureau (“CFPB”) issued a bulletin about third party vendors. In October 2012, the Federal Financial Institutions Examination Council (“FFIEC”) issued a guidance on IT service providers. The Federal Deposit Insurance Corporation (“FDIC”) joined the regulatory bandwagon with its September 2013 Financial Institution Letter regarding payment processing relationships with high risk merchants. The Board of Governors of the Federal Reserve System (“Federal Reserve Board”) followed shortly thereafter with a Guidance on Managing Outsourcing Risks in December 2013.

---

Financial institutions may not always be able to seek indemnification for non-compliance with regulatory requirements by their service providers. Recent CFPB actions raise the possibility that financial institutions could be barred from receiving indemnification under certain circumstances.\textsuperscript{6} In another example, both a bank and service provider were sued in 2008 when the FDIC and the Federal Trade Commission (“FTC”) joined forces against CompuCredit Corp. and Synovus Financial Corp. for deceptive credit card marketing practices in an unprecedented act of regulatory cooperation. So, it’s clear that stakes are going up not only for financial institutions but also service providers.

Mobile Payments Legal Issues: A Primer

Introduction ................................................................................................................... 3
Payments Regulation .................................................................................................... 5
Transactional Issues ..................................................................................................... 7
Unfair or Deceptive Acts or Practices ......................................................................... 9
Bank Secrecy Act / Anti-Money Laundering Regulations ........................................ 11
Money Transmission ................................................................................................... 13
Remittance Transfers ................................................................................................. 15
Cross-Border Issues ................................................................................................. 16
Financial Privacy ........................................................................................................ 18
Big Data ....................................................................................................................... 21
Data Security ............................................................................................................... 23
Patent and Intellectual Property .............................................................................. 25
Litigation and Enforcement Actions ......................................................................... 26
Virtual Currencies and Other Emerging Payments ................................................ 28
Introducing **MoFoMobl$** (or MobileMoney), Morrison & Foerster’s **free app** for the mobile payments industry. MoFoMobl$ provides a regulatory overview of key issues and considerations, access to timely alerts and articles, and a weekly news digest on market developments. It’s like having a lawyer on your staff, but not on your payroll….  

The technological capability of smartphones has increased dramatically over the past few years, spawning a revolution in the mobile payments industry. Use MoFoMobl$’s library of selected expert issue overviews to stay informed about the key regulatory issues and considerations critical to the mobile payments industry. You will have one-touch access to each topic using MoFoMobl$’s user-friendly interface on your mobile device.

MoFoMobl$ provides quick access to MoFo’s collection of Client Alerts and articles written by our MoFo lawyers focusing on key developments in the mobile payments industry, including developments from federal agencies, legislative updates, consumer trends, and more. MoFoMobl$ also features push service notifications, allowing you to receive new alerts right on your home screen.

The app includes our frequently updated resource index, the News Roundup, with links to the latest press releases, news, online articles, and commentary on mobile and emerging payments issues. Each week, links to these publicly available updates are loaded right to your mobile device. You will also have access to our regulatory tracking tools, quick access to contact information for mobile payments experts, and a description of our Financial Technology Practice.

To download our app, click here, or visit www.mofo.com/resources.
• Access a variety of legal and business issues critical to the mobile payments industry.
• Read related MoFo Client Alerts without leaving the app.
• Receive notifications when a new alert is published, right on your screen.
• View third-party articles to keep abreast of news and trends.
• Always smart, friendly, and free.
• **Technological Evolution.** The technological capability of smartphones and other portable handheld electronic devices capable of accessing the Internet has increased dramatically over the past few years. This technological evolution in functionality has not only led to the development of new ways for consumers to engage in traditional banking transactions (e.g., depositing a check through remote deposit capture), but also has spawned a revolution in the payments industry by establishing new channels through which consumers can make payments and merchants can take payments.

• **What Are Mobile Payments?** The term “mobile payments” captures a broad range of payment-related activities. Many of these activities typically provide consumers or merchants with one or more of the following functionalities: (1) the ability to process payments for goods and services; (2) the storage of payment instruments, coupons, and/or rewards, and the enabling of payment services; and (3) the ability to facilitate peer-to-peer transfers. The variety of payment options available to consumers is growing every day, and is an exciting development in the payments business. While mobile payments providers may facilitate multiple payment service functions, most offer products that fall within common product categories.

---

**KEY POINTS**

**Mobile Payments Marketplace**

• **Mobile Wallets.** Applications on mobile devices can create a mobile wallet that allows a consumer to pay for products or services with stored payment credentials. These apps may have prepaid functionality similar to general-use reloadable prepaid cards. This mobile payment functionality can be employed by various technologies, the most common of which include near-field communications, radio-frequency identification or quick-response codes.

• **Mobile as Point-of-Sale.** Mobile devices configured to become point-of-sale terminals can allow almost any person to accept and process payments. This mobile payments function is commonly associated with handheld devices that are fitted with a card-reader attachment.

• **Mobile Payments Platform.** Apps that create a payments platform can allow a consumer to transfer funds between parties even without a purchase or sale. This mobile payments function is often used to facilitate the peer-to-peer transfer of funds.

• **Closed-Loop Payments.** Payment-related apps also can allow a consumer to make payments through a merchant- or subscriber-based platform. This mobile payments function may require a consumer to load funds into the platform and operates in a manner similar to that of a prepaid card.

• **Carrier Billing.** Telecommunications carriers that provide a direct carrier billing service can allow a consumer to make purchases using their mobile device and charge their carrier account. This mobile payments function can operate without a consumer needing to use or link to a separate financial instrument, such as a credit card or debit card.
• **Legal Framework.** Although the legal framework for mobile payments is evolving, the relative newness of mobile payments as a technology has generated questions regarding the regulatory treatment of such payments, as well as questions regarding the roles and responsibilities of the various participants in a mobile payments transaction. The goal of this primer is to give context to the many issues that can arise in the mobile payments ecosystem and to provide a framework for considering these issues.

And, payments are just one part of the equation. The ubiquity of smartphones in the hands of consumers also enables new ways for consumers and businesses to connect through geolocation information and targeted advertising. The confluence of technological and marketing developments relating to smartphones has captured the attention of policymakers and generated a regulatory “buzz” about mobile payments.

**Legal Considerations**

• **Existing Laws Apply Despite New Technology.** Although mobile payments providers are at the cutting edge of financial services innovation and are developing products using the newest forms of technology, these new ways of conducting payment and other transactions remain subject to the existing set of laws and regulations governing payment providers, financial products and payment transactions.

• **Rules Are Evolving.** Currently, there is no single law or set of laws governing mobile payments or all of the entities operating within the mobile payments ecosystem. The simple fact is that most existing statutes and regulations governing payments never contemplated the use of mobile payments. Consequently, the various federal and state agencies that share rulemaking and enforcement responsibilities for consumer-facing businesses have been evaluating how mobile payments are governed under existing laws and regulations and whether amendments to such laws are necessary.

• **Scope.** This primer focuses primarily on legal considerations that can arise under U.S. laws and regulations. Nevertheless, it is important to recognize that the enablement of mobile payments triggers additional questions about jurisdictional issues and the applicability of international laws. For example, payment functionality that is accessed by non-U.S. residents or enabled in countries outside the U.S. may implicate international laws and regulations. These issues should be thoroughly vetted by mobile payments providers when developing product functionality, terms of service and agreements with other payments system participants.
Payments Regulation

- **Regulatory Environment.** Despite the lack of a single law or set of laws and regulations governing mobile payments, the provision of mobile payments still generates regulatory issues under existing federal and state consumer protection statutes.

Laws and regulations potentially affecting mobile payments providers are vast, and multiple regulatory agencies share responsibility for regulating the mobile payments marketplace. The Consumer Financial Protection Bureau ("CFPB") is responsible for administering federal consumer financial laws, including laws applicable to payment transactions and the entities that process or facilitate such transactions. The Federal Trade Commission ("FTC") has a broad consumer protection mandate and extensive enforcement authority over non-banks under Section 5 of the Federal Trade Commission Act. In addition, various state banking agencies regulate money transmissions businesses. Although other regulatory agencies also have authority to regulate aspects of the payments ecosystem, such as the Federal Reserve Board and its authority to regulate interchange fees, the CFPB and the FTC are especially focused on understanding payment-related activities and on how the various entities that perform those activities operate.

**KEY POINTS**

**Regulatory Considerations**

- **Regulation E.** Regulation E, which implements the Electronic Fund Transfer Act ("EFTA"), establishes the basic rights, responsibilities and liabilities of consumers and entities that use and/or provide electronic fund transfer ("EFT") services. Regulation E applies to entities that hold consumer asset accounts and provide EFT services using those accounts. Regulation E also may apply to an entity that provides a consumer with an access device to make EFT transfers regardless of whether the entity also holds the consumer's account. For example, mobile payments providers who issue access devices and facilitate or initiate the transfer of funds through an electronic terminal, telephone or computer for the purpose of ordering, instructing or authorizing a financial institution to debit or credit a consumer's account may be required to comply with Regulation E rules.
  - **Error Resolution under Regulation E.** Special error resolution procedures for consumers are required under Regulation E. Mobile payments providers covered by Regulation E must provide consumers with the ability to dispute billing errors, and must investigate alleged errors promptly.

- **Regulation Z.** Regulation Z, which implements the Truth in Lending Act, applies to consumer open-end credit, such as credit cards, and establishes requirements for credit card issuers at various stages of the consumer credit life cycle. Mobile payments providers who provide payment products or services in connection with a credit card may be subject to Regulation Z requirements, such as providing consumers with mandated account-opening disclosures, periodic statements and billing error resolution rights.
Error Resolution under Regulation Z. Special error resolution procedures for consumers are mandated by Regulation Z. Mobile payments providers covered by Regulation Z must provide consumers with the ability to report billing errors, and must investigate and resolve the dispute within a limited time period.

- Regulation II. Regulation II implements the EFTA with respect to debit interchange fees, payment card network exclusivity, and debit card transaction routing. These rules apply to the fees that a card issuer in a four-party network may receive in connection with a debit card transaction. Mobile payments providers must consider whether their debit card products or services are subject to Regulation II and, if so, whether their products or services are in compliance with Regulation II fee restrictions, the routing and exclusivity requirements, and other limitations. Mobile payments providers should be mindful that Regulation II prohibitions on circumvention and evasion apply broadly and may have implications for mobile payments providers who compensate debit card issuers.

- Payment Processors and Service Providers. The Bank Service Company Act provides the federal banking agencies with the authority to regulate services performed for regulated financial institutions. Under the Dodd-Frank Wall Street Reform and Consumer Protection Act, a service provider is defined as any person that provides a “material service” to a covered person in connection with the offering or provision of a consumer financial product or service. Mobile payments providers who are viewed by federal banking regulators as performing a “material service” for banks may be subject to regulatory scrutiny by the CFPB, a federal banking agency and/or the FTC.
Mobile payments products and services are being designed and implemented through strategic partnerships with financial institutions, payment card networks, merchants and technology companies. Mobile payments providers who enter into contractual agreements with other entities should consider the following transactional issues.

**KEY POINTS**

**Transactional Considerations**

- **Program Descriptions.** In agreements involving mobile payments providers, a detailed description of the program and agreement is critical to defining the responsibilities and obligations of the participating parties. The agreement should clearly define the scope of the contemplated arrangement and the nature and extent of the product offering, including which entity will operate as the end-user service provider and/or whether the agreement between a mobile payments provider and payment network covers credit cards, debit cards, prepaid cards and/or checking accounts.

- **Value Proposition and Program Economics.** Mobile payments providers must also address the value propositions offered to mobile payments customers. Certain value propositions that may differ from the traditional arrangements—loyalty programs, mobile app coupons or gift cards sent to a mobile device—may implicate different legal requirements for the various participants, particularly if these value propositions have different funding sources. In this regard, parties to any agreement should also address the various economic considerations of products being offered, such as premium cards vs. plain vanilla cards, prepaid vs. credit, as well as whether payment is by per account or per mobile device.

- **Program Expenses.** Parties to an agreement should identify all expenses associated with the program, including all operational and marketing costs associated therewith. The parties should clearly identify the scope of such expenses and the specific parties responsible for such expenses.

- **Merchant Relationships.** Parties to an agreement should address the types of incentives offered to merchants to encourage mobile payments acceptance, as well as the allocation of costs between the parties associated with those merchant incentives.

- **Customer Data Ownership.** Parties to an agreement should address the ownership of customer information among the parties to the agreement (e.g., bank, merchant, processor, and potentially mobile carrier, depending on deal structure), including any overlap of information ownership, since consumers could be viewed as customers of multiple parties to the program.

- **Data Security.** Parties to an agreement should address the respective roles and responsibilities of the parties regarding data security and the collection, storage and protection of consumer data.
- **Intellectual Property.** Parties to an agreement should include provisions specifying the ownership of intellectual property, particularly new intellectual property that is jointly developed by the parties in connection with the program, such as the joint development of new mobile apps for the program, use of trademarks, the linkage of mobile apps to social media, or posts to social media Web sites after a customer makes a purchase using mobile payments featuring a particular merchant.

- **Compliance with Applicable Law.** Parties to an agreement must address legal compliance responsibilities by identifying the laws and regulations that apply to the product, the type of customer information that is handled and rules for advertising and marketing. Agreement provisions should clearly delineate which party is responsible for compliance functions and also address requirements for maintaining and following written policies and procedures to comply with applicable law.

- **Indemnification and Liability.** Parties to an agreement must address their respective indemnification obligations, as well as responsibility for billing disputes, unauthorized use and fraud under Regulation Z and other payment network regulations.

- **Reporting.** Parties to an agreement should include provisions detailing any reporting obligations the mobile payments provider may owe to other parties, including merchants, issuers and payment networks.
Unfair or Deceptive Acts or Practices

• **Regulatory Authority.** Innovation in the mobile payments marketplace can lead to new and better ways to deliver payment services. At the same time, companies that innovate should consider the federal and state laws regulating certain practices. For example, federal laws—against unfair or deceptive acts or practices (“UDAP”) found in Section 5 of the Federal Trade Commission (“FTC”) Act, and against unfair, deceptive or abusive acts or practices (“UDAAP”) found in Title X of the Dodd-Frank Act—shape and/or limit the practices of mobile payments providers. Additionally, laws in most states mirror the federal UDAP statutory scheme and may impose another set of potential restrictions.

• **Enforcement.** Mobile payments providers that engage in UDAPs or UDAAPs may be subject to enforcement action by the Consumer Financial Protection Bureau (“CFPB”), the federal banking agencies and/or the FTC at the federal level, as well as by state attorneys general and/or private plaintiffs at the state level. UDAP and UDAAP issues in mobile payments can arise in a variety of ways, and may include claims with respect to the clarity and sufficiency of required disclosures, pricing or fees, payment authorization, recurring payments, negative options, free-to-pay conversions, dispute resolution and information collection, use and sharing practices.

---

**KEY POINTS**

**Trade Practices Considerations**

• **Federal and State Laws.** Practices that mislead reasonable consumers to their detriment, might be considered to be “deceptive.” Practices that cause unavoidable harm to consumers—such as debiting a consumer’s account without his or her authorization—might be considered to be “unfair.” “Abusive” practices are defined as those which take advantage of a consumer’s lack of understanding or inability to protect his or her own interests. The CFPB has authority to prescribe rules prohibiting UDAAPs—including “abusive” acts or practices—under Section 1031 of the Dodd-Frank Wall Street Reform and Consumer Protection Act. The FTC and the federal banking agencies have UDAP enforcement authority, and the banking agencies often rely on FTC guidance in this regard. Additionally, mobile payments providers are subject to state UDAP laws that typically mirror federal UDAP rules.

• **Federal Banking Agency Enforcement.** Mobile payments providers that are supervised by the CFPB or a federal banking agency should consider the UDAP or UDAAP enforcement practices of their particular regulatory agency(s). Under Section 8 of the Federal Deposit Insurance Act, federal banking agencies may pursue UDAP enforcement actions against institutions they supervise. Recent UDAP enforcement actions by the Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation demonstrate that supervised banking entities continue to be scrutinized by their bank regulatory agencies for UDAP compliance. The CFPB may also pursue enforcement actions for UDAAP violations in connection with the offering or sale of any consumer financial product or service.
• **FTC Enforcement.** Mobile payments providers should consider the risks presented by the FTC’s enforcement actions and its public statements regarding how companies may avoid a UDAP charge. Recent actions against technology companies emphasize the FTC’s focus on ensuring that consumers are given adequate notice and the ability to provide consent prior to authorizing mobile and online transactions.

• **State Enforcement.** Mobile payments providers should consider the UDAP risks presented by both state authorities and private plaintiffs. State attorneys general may pursue enforcement actions for violation of state UDAP laws. Some state laws also provide private plaintiffs with private rights of action. In either case, a regulator or plaintiff may be able to seek injunctive relief, civil money penalties and/or redress against mobile payments providers alleged to violate state UDAP laws.
• Under federal law, both banks and non-banks are subject to the reporting and recordkeeping provisions of the Bank Secrecy Act ("BSA") and its implementing regulations, including the principal requirement to implement an effective anti-money laundering ("AML") program. Non-bank entities, such as money transmitters, currency exchangers, or providers or sellers of prepaid access, may be classified as money services businesses ("MSBs") and, thus, subject to the BSA. As a result, non-bank mobile payments providers still may be subject to BSA requirements if they are classified as MSBs.

KEY POINTS

BSA/AML Considerations

• **Registration.** MSBs must register with the Treasury Department’s Financial Crimes Enforcement Network ("FinCEN"). This registration must be renewed every two years.

• **Agent List.** MSBs must maintain a list of their agents, and FinCEN can request a copy at any time. Agents need not separately register with FinCEN.

• **Report Filing.** MSBs must file various reports associated with certain transactions or suspicious activities, including Suspicious Activity Reports and Currency Transaction Reports. Each report is triggered by particular circumstances, requires the filing of specific information, and is accompanied by obligatory recordkeeping requirements.

• **AML Programs.** Mobile payments providers subject to the BSA will be required to develop, implement, and maintain an effective AML program that is commensurate with the risks posed by the nature of their business. Compliant AML programs generally include: (1) policies, procedures and internal controls reasonably designed to assure ongoing compliance with the BSA, as well as BSA training for appropriate personnel and a designated BSA Compliance Officer; (2) independent review and auditing of the AML program; and (3) observance of specified certain customer identification and recordkeeping standards.

• **Enforcement.** BSA and AML requirements are designed to prevent fraud in the payments system, as well as to prevent money laundering and terrorist financing activities. Mobile payments providers may be viewed with suspicion by traditional bank regulators given their non-bank status and the BSA/AML implications of their operations. Any efforts by federal bank regulators to prevent banks from processing transactions for mobile payments providers, under the auspices of preventing fraud, safety and soundness or other regulatory purposes, could severely impair the business activities of mobile payments providers. Additionally, non-compliance with BSA or AML requirements can result in civil and criminal penalties, including significant fines, as well as criminal liability for the acts of employees.
• **Office of Foreign Assets Control.** The Treasury Department administers and enforces economic and trade sanctions through its Office of Foreign Assets Control ("OFAC"). OFAC administers U.S. sanctions laws, such as the Trading With the Enemy Act and the International Emergency Economic Powers Act. OFAC acts to prevent certain prohibited transactions, such as trade, financial transactions or other dealings with certain countries, businesses, and individuals. OFAC regulations also require businesses to identify and freeze the assets of targeted countries and Specially Designated Nationals. OFAC mandates that U.S. individuals and entities screen for these countries, businesses, and individuals, but does not require implementation of a specific compliance program.

**OFAC Considerations**

- **Compliance Program.** Even though OFAC does not mandate implementation of a specific sanctions compliance program, developing a risk-based OFAC compliance program is in a mobile payments provider’s best interests.

- **Criminal and Civil Penalties.** U.S. sanctions laws impose strict criminal and civil liability, meaning that companies can be prosecuted for even unintentional violations, and the fines can be substantial.

- **Enforcement.** Federal regulators and prosecutors will consider the effectiveness of a company’s OFAC screening program when deciding whether to prosecute or impose fines and/or other penalties.
Money Transmission

• **Federal Law.** Under the Bank Secrecy Act (“BSA”), entities that are engaged in a “money services business” are subject to certain federal law requirements. Money services businesses include entities that are “providers” or “sellers” of “prepaid access” (i.e., access to funds that have been paid in advance and can be retrieved or transferred in the future), as well as entities that are engaged in “money transmission services” (i.e., money transmitters). Whether an entity is a money transmitter under federal law is based on facts and circumstances, but the definition is broad, and includes the acceptance of the currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means, as well as entities engaged in the transfer of funds.

• **State Money Transmission Laws.** The growth in use of mobile payments products and services has attracted the regulatory scrutiny of state regulators. Forty-eight states and the District of Columbia have statutes requiring a license to engage in money transmission activities, which can include certain mobile payments activities. These are primarily safety and soundness laws intended to protect senders and recipients of funds and, as such, are also consumer protection statutes. As virtual marketplaces continue to develop and expand, state regulators are faced with emerging technologies and commercial arrangements that challenge traditional interpretations of state licensing laws.

### KEY POINTS

#### Licensing Requirements

• **State Licensing.** Whether a state licensing requirement applies to a mobile payments provider and its activities depends on a particular state’s statute and regulations (if any). The licensing process is complex and time consuming and requires the submission of highly detailed business plans and personal information about the individuals involved in overseeing the licensed activity.

• **Federal and State Enforcement.** State banking and other agencies have the authority to regulate money transmitters, pursue enforcement actions, and impose civil penalties against entities in violation of state money transmission laws and licensing requirements. Federal enforcement is also available since it is a violation of federal law to engage in money transmission activities without a required state license.

• **Federal Registration and Requirements.** A money services business under federal law must register with the Financial Crimes Enforcement Network. In addition, the BSA requires that entities engaged in money services businesses implement certain anti-money laundering requirements, including adoption of an anti-money laundering program, observance of certain customer identification and recordkeeping standards, and ongoing reporting of suspicious activity.
• **State Licensing.** The process to become a licensed state money transmitter is complex and can take more than a year to complete. It is often necessary to become licensed in all states and territories, which can result in significant cost expenditure. Whether a state’s licensing requirement applies to mobile payments services will depend on a particular state’s statute and regulations. However, activities that trigger licensing requirements in particular states are often broadly defined.

License applications require the preparation and submission of highly detailed and often confidential information. A wide range of personal information (e.g., financial information, fingerprints) from officers, directors, and other persons responsible for overseeing a business also is required. In addition, most states require that a bond be posted as a condition of granting a license.

• **Enforcement.** There are civil and criminal penalties on both the state and federal level for operating a money transmission business without a license. State money transmitter laws provide a wide array of civil penalties for operating without a license. These include civil fines and suspension or revocation of a licensee’s or an agent’s license to operate.

In many states, operating without a license also constitutes a crime. These criminal violations are charged either as felonies (e.g., California) or misdemeanors (e.g., New York). Operating without a required state money transmitter license also is a felony under federal law, punishable by fines, up to five years in prison, or both.
Remittance Transfers

- Remittance transfers are electronic transfers of money from U.S. consumers to recipients in foreign countries. Regulation E, which implements the Electronic Fund Transfer Act, requires companies, including banks, engaging in remittance transfer services to provide certain disclosures and undertake error resolution procedures with respect to remittance transfers. The Consumer Financial Protection Bureau ("CFPB") remains active in its regulation of remittance transfers and has issued proposed rules to subject certain non-bank money transfer providers to CFPB supervision and examination as "larger participants." Accordingly, mobile payments providers who facilitate cross-border transactions should consider whether they are subject to remittance transfer requirements under Regulation E and whether they will be subject to supervision and examination by the CFPB.

**KEY POINTS**

**Selected Remittance Transfer Provisions**

- **Disclosures.** Remittance transfer providers must provide to each "sender" of a remittance transfer a prepayment disclosure and a receipt showing, among other information, the exchange rate used and the amount of money in the currency to be received by the recipient of the transfer.

- **Error Resolution.** Remittance transfer providers must allow senders to dispute errors for up to 180 days following a remittance transfer. If a remittance transfer provider receives notice that an error occurred from a sender within 180 days of the promised delivery date of the remittance transfer, the provider must, within 90 days, conduct an investigation. The provider must report the results of the investigation to the sender within three days of completion.

- **Right of Cancellation and Refund.** Remittance transfer providers must afford senders a 30-minute cancellation period after a sender pays for a remittance transfer. Special rules apply for transfers scheduled at least three business days prior to the date of transfer.
Cross-Border Issues

- Mobile devices traverse international borders as often as the consumers and merchants who carry these devices. Certain cross-border legal issues may arise when consumers or merchants engage in mobile payments transactions across international borders. For example, there may be legal uncertainty as to the laws that govern a particular mobile payments transaction. As a result, mobile payments providers should be mindful of two issues arising out of cross-border transactions. The first is whether U.S. payment laws generally apply to the transaction and parties. If U.S. laws apply, the second issue is which U.S. laws govern cross-border payment transactions.

- For parties who transact payments using a mobile payments product or service abroad, whether the transaction is covered by U.S. payment laws depends on the specific facts and circumstances. Regulatory agencies responsible for ensuring compliance with payment laws typically evaluate a variety of facts and circumstances surrounding the transaction to determine whether U.S. payment laws apply to cross-border payments, including where the account was opened, where the consumer resides, and where the funds in the transaction are sent from. In circumstances where U.S. laws do apply to cross-border mobile payments transactions, mobile payments providers who engage in these transactions may be subject to federal laws that regulate cross-border payments, including Financial Crimes Enforcement Network wire transfer rules, remittance transfer rules and BSA/AML rules.

### KEY POINTS

#### Cross-Border Payment Laws

- **Wire Transfers.** The Bank Secrecy Act ("BSA") requires financial institutions to obtain and include certain information on wire funds transfers and transmittal of funds. Under the BSA, the FinCEN “Travel” rule requires financial institutions to pass on information about the transmitter and the recipient of funds to the next financial institution in connection with wire transfers involving more than one financial institution.

- **Remittance Transfers.** Under Regulation E, companies enabling consumers to electronically transfer funds abroad (remittance transfers) are required to provide certain disclosures and error resolution procedures for those remittance transfers. For cross-border remittance transfers made electronically or by mobile phone, Regulation E specifies that the location of a “sender” is determined by the payment provider based on the information provided by the sender. Thus, whether the remittance transfer requirements apply to a mobile payments transaction may be determined by the specific facts and circumstances surrounding the location of the transaction’s origination, the location of the recipient, and where the funds are transferred from.

- **BSA/AML.** Both banks and non-banks are subject to the reporting and recordkeeping provisions of the BSA and its regulations, including the requirement to implement an anti-money laundering ("AML") program. Non-bank entities also can be subject to the BSA if classified as money services businesses, such as money transmitters, currency exchangers, or providers or sellers of
prepaid access. Whether mobile payments providers are subject to BSA/AML reporting and recordkeeping requirements may depend on whether they are classified as non-bank entities engaged in money services transactions.
Financial Privacy

- Mobile payments providers that provide financial products or services to consumers or that provide services to financial institutions may be subject to the requirements of the Gramm-Leach-Bliley Act ("GLBA") and the Fair Credit Reporting Act ("FCRA"). These federal financial privacy laws regulate the collection, use and disclosure of consumer financial data. The requirements of the GLBA and the FCRA can apply to mobile payments providers, even those engaged in "non-traditional" financial services.

KEY POINTS

Financial Privacy Considerations

- **Financial Institutions and Service Providers.** The GLBA generally requires that a "financial institution" provide a consumer with a privacy notice and opportunity to opt out before the financial institution discloses financial information about the consumer to a nonaffiliated third party. Federal law broadly defines the types of entities that are considered financial institutions. A mobile payments provider who is engaged in processing, storing and transmitting financial data may be considered a financial institution subject to the requirements of the GLBA. Even if a mobile payments provider is not considered a financial institution, however, it may nonetheless be covered by GLBA requirements if it receives consumer financial information from a financial institution in order to provide services to the financial institution.

- **Credit Reporting Agencies, Furnishers and Users.** The FCRA regulates the collection, use and disclosure of credit report information (i.e., information that is or may be used to determine a consumer’s eligibility for credit, insurance, employment and other statutory "permissible purposes"). Entities engaged in activities covered by the FCRA may be considered credit reporting agencies, users of credit reports and/or furnishers of information to credit reporting agencies, and subject to specific requirements and limitations with regard to the use and disclosure of consumer data.

- **Financial Institutions and Service Providers**
  - A mobile payments provider should consider whether engaging in its mobile payments business would cause it to be considered a "financial institution" for purposes of the GLBA. If a mobile payments provider is providing financial products or services—including mobile payment services—directly to consumers, the mobile payments provider may be required to comply with GLBA privacy requirements, including:
    - Providing its consumer customers with initial and annual GLBA privacy notices; and
    - Providing its consumer customers with an opportunity to opt out of (i.e., limit) the sharing of information about them with nonaffiliated third parties. There are some exceptions to the sharing restrictions in the GLBA. For example, the GLBA
specifically permits data to be shared with nonaffiliated third parties to process or service customer transactions, to prevent fraud or for law enforcement or regulatory purposes.

Moreover, under the GLBA, a mobile payments service provider would be required to limit its own use and disclosure of consumer financial information received from companies to which the mobile payments provider provides services. Specifically, the mobile payments service provider would only be permitted to use and disclose such information in order to perform its service function.

- **Credit Reporting Agencies, Furnishers and Users**
  - A mobile payments provider should consider the potential application of the FCRA to its business. Where a mobile payments provider obtains credit reports or similar data from vendors for the purpose of determining a consumer’s eligibility for credit, insurance, employment or other “permissible purposes,” it may be subject to the FCRA. If a mobile payments provider is deemed to be subject to the FCRA, it must comply with specific requirements depending on the activities in which it is engaged.

**FCRA Requirements and Duties**

- **Credit Reporting Agencies.** Credit reporting agencies are companies that collect data about consumers and assemble reports to be used by businesses to make credit, insurance, employment and similar decisions about consumers. Credit reporting agencies have numerous statutory obligations, including requirements regarding the content of credit reports, the investigation of consumer disputes, and the prevention of fraud and identity theft.

- **Furnishers.** Companies that furnish consumer information to credit reporting agencies for inclusion in credit reports have various obligations, including requirements relating to the accuracy of the information furnished to credit reporting agencies and the investigation of consumer disputes.

- **Users.** Companies that obtain credit reports from credit reporting agencies may only use such credit reports for specified “permissible purposes,” and have various other obligations, such as providing notice to consumers when a credit report was used to take an action adverse to the consumer.
  - A mobile payments provider also should consider the limitations the FCRA imposes on the sharing of consumer information among affiliates and the use of information shared among affiliates for marketing purposes, and whether the mobile payments provider would be required to provide consumers with notice and an opportunity to opt out of such sharing or use of information shared among affiliates for marketing purposes.

- **State Financial Privacy Laws**
  - A mobile payments provider also should consider whether it is subject to the requirements of any state privacy law, such as the California Financial Information Privacy Act (“CFIPA”) or the California Online Privacy Protection Act (“CalOPPA”).
    - The CFIPA is similar to the GLBA, but it requires that financial institutions obtain consent (i.e., opt in) for disclosures of customer data to nonaffiliated third parties. The CFIPA also requires financial institutions to provide customers with the opportunity to opt out of disclosures of their information to affiliated companies, and opt out of joint marketing campaigns with other financial institutions.
If the mobile payments provider maintains a Web site or a mobile phone app that is accessible by California residents, the mobile payments provider should consider whether it must comply with the CalOPPA requirement to post on its Web site or mobile app a privacy policy addressing its information handling practices related to the information that it collects from individuals through the Web site or app.
• **Non-Financial Privacy Laws.** Currently, there is no overarching federal privacy law in the U.S. governing the collection, management and use of non-financial information collected and consolidated in the payment transaction process. Existing federal privacy statutes and regulations are narrowly tailored toward a particular entity, sector or purpose, and are not designed to address services provided and information maintained by mobile payments providers. The Federal Trade Commission (“FTC”), however, has asserted jurisdiction generally over the collection, use and sharing of personal information. In addition, the nature of the mobile payments business could subject a mobile payments provider to a variety of privacy laws and requirements, including the Telephone Consumer Protection Act (“TCPA”) and Section 5 of the FTC Act.

### KEY POINTS

**Big Data Legal Considerations**

- **TCPA.** The TCPA regulates the autodialed delivery of marketing and non-marketing calls and text messages. The TCPA provides consumers with the ability to recover statutory damages of up to $1,500 per violation, which has led to an explosion of TCPA class action lawsuits, typically alleging that the necessary consent to deliver a call or text message was not obtained.

- **FTC Act.** “Unfair” or “deceptive” data collection, use and sharing practices can be subject to enforcement by the FTC through Section 5 of the FTC Act. As more and more consumers engage in online and networked activities using their mobile devices, the FTC has studied how companies collect and use data in the mobile app ecosystem, as well as the disclosures they make about that collection and use, and it has made recommendations intended to help companies avoid a charge of unfairness or deception.

- **Emerging Big Data Privacy Concerns.** Growth in the number of companies involved in the mobile payments marketplace has given rise to renewed privacy concerns by policymakers. Both policymakers and consumers have grown concerned about the large amount of detailed personal information collected, used and stored by private companies, as well as by the federal government. In this regard, the following issues have been identified by policymakers as areas of particular concern.

### Big Data Privacy Considerations

- **Interest-Based Advertising.** Interest-based advertising, whereby a company tracks a consumer’s activities over time and across Web sites, apps or other properties in order to deliver advertising targeted to the consumer’s perceived interests, has attracted the interest of the FTC and other agencies and generally requires enhanced notice and choice. Mobile payments providers—as well as service providers delivering targeted advertising, coupons or other offers to
app users based on their activities on other Web sites, apps or properties—may be considered to be engaged in interest-based advertising and could become the target of future legislation or enforcement actions.

- **Geolocation and Tracking.** Use of consumer data generated from online and offline mobile device activity has drawn the attention of privacy advocates and Congress. Although businesses collecting and using such data do not currently have specific statutory guidance for their activities, regulatory agencies and legislatures have proposed numerous changes to existing laws to address privacy issues related to the collection of precise geolocation information and mobile tracking practices. The FTC has made it clear that the collection of precise geolocation information without just-in-time notice and opt-in consent may be an unfair and/or deceptive practice under Section 5 of the FTC Act, including, for example, if the collection, use or disclosure of the information is not reasonably expected by the consumer under the circumstances.

- **Mobile Devices and Payments.** Mobile payments providers who collect or manage consumer information face a challenging legal landscape in which future rules may impose requirements affecting current business operations. Policymakers—concerned about the large amount of detailed personal and purchase information collected and consolidated by mobile payments providers—have called for federal privacy laws that expressly address mobile payments privacy issues.
Data Security

- Mobile payments providers that maintain, use, disclose or otherwise handle personal information relating to consumers, including, for example, financial account numbers, may be subject to a wide variety of data security requirements under federal and state law and by contract.
  
  - **GLBA.** The Gramm-Leach-Bliley Act ("GLBA") imposes data security requirements on financial institutions. A mobile payments provider should consider whether engaging in its mobile payments business would cause it to be considered a "financial institution" for purposes of the GLBA. If a mobile payments provider is deemed to be a financial institution for purposes of the GLBA, the mobile payments provider would be subject to data security rules issued by a GLBA regulator. If the mobile payments provider is not a bank, insurance company or broker dealer, the company’s GLBA regulator is likely to be the Federal Trade Commission ("FTC"), and the mobile payments provider would be subject to the FTC’s Safeguards Rule.

  - **FTC Act.** Section 5 of the FTC Act prohibits unfair or deceptive acts or practices in or affecting commerce. The FTC has used its authority under the FTC Act to bring enforcement actions against companies for failing to appropriately protect personal information relating to consumers.

  - **State Laws.** If a mobile payments provider handles personal information relating to consumers, it may be subject to at least two types of state data security laws: (1) laws that require companies to safeguard or protect personal information, and (2) laws that require companies to notify consumers and others of breaches of the security of personal information.

  - **PCI DSS.** If a mobile payments provider is handling payment card information, it may be contractually required to comply with the Payment Card Industry Data Security Standard ("PCI DSS"), the payment card industry’s security standards for payment card information. For example, if a mobile payments provider enters into a contract with a merchant bank or payment card network regarding the acceptance or processing of payment card transactions, the contract likely will require that the mobile payments provider comply with the requirements of PCI DSS.

  - **Contractual Considerations.** If a mobile payments provider handles personal information relating to consumers in connection with providing services to another company, the mobile payments provider may be subject to contractual requirements to protect the personal information.

---

**KEY POINTS**

**Mobile Payments Marketplace**

- **GLBA Requirements.** The FTC’s Safeguards Rule requires that financial institutions subject to the FTC’s GLBA authority maintain security measures to protect customer information. For example, the Safeguards Rule requires that financial institutions develop, implement and maintain
written, comprehensive information security programs to protect customer information, conduct risk assessments and design and implement safeguards to control identified risks, and require service providers by contract to implement and maintain these safeguards.

- **FTC Act.** The FTC has made it clear, through public pronouncements and enforcement actions, that companies must have “reasonable” security measures in place to protect personal information relating to consumers. The failure to protect personal information may be deemed “unfair” under Section 5 of the FTC Act. Also, companies that make public representations (e.g., in their privacy policies) about the security measures they have in place may be subject to enforcement under Section 5 for making deceptive statements if they do not have in place security measures consistent with those public representations.

- **FFIEC Guidance.** If a mobile payments provider is a bank or credit union, the mobile payments provider may be subject to a wide variety of guidance issued by federal bank regulators regarding data security, including guidance relating to the authentication of customers who obtain financial products and services online.

- **State Safeguards Laws.** A number of states have enacted laws requiring that companies protect personal information relating to consumers. Some laws are general in nature and require that companies maintain reasonable security measures to protect personal information. Other laws, such as those in Massachusetts, Nevada and Oregon, require that companies take specific and detailed security measures, such as encrypting personal information.

- **State Security Breach Notification Laws.** Forty-seven states, the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands have enacted laws that require companies to provide notice to consumers and others in the event of a data breach. If a mobile payments provider experiences a security incident involving consumer personal information, the mobile payments provider may have obligations under these state breach laws.

- **Contractual Requirements.** A mobile payments provider that handles payment card information or that provides services to other companies should consider its various contracts to determine whether such contracts impose any data security requirements on the mobile payments provider, such as, for example, requiring compliance with PCI DSS.
Growth or innovation in any technology-oriented marketplace invariably produces a complex web of intellectual property considerations. The mobile payments market is no different, since approximately 20,000 patents presently exist for the mobile wallet product type alone. To avoid unanticipated costs and litigation, mobile payments providers developing and bringing mobile payments products to market should consider steps to patent their innovations and should be aware of, and prepared for, potential infringement claims. A sound legal strategy for managing exposure to intellectual property claims takes into account both freedom to operate issues and indemnification assurances.

**KEY POINTS**

**Intellectual Property Considerations**

- **Freedom to Operate.** Intellectual property infringement claims against mobile payments providers, from either existing service providers or intellectual property trolls, may result from unforeseen intellectual property restrictions. In this regard, a service provider who sues for infringement may accept a mobile payments provider as a customer while an intellectual property troll is unlikely to do so.

- **Indemnification.** Obtaining indemnification assurances may give a business the ability to shield itself against future infringement claims; for example, mobile payments providers subject to licensing or use of intellectual property may obtain indemnification from service providers against other infringement claims by trolls or other competitors.

- **Trademarks.** Developing a brand through the use of trademarks and avoiding infringement claims are also aspects of intellectual property that should be considered by mobile payments providers before introducing a new mobile payments product or service. For example, trademark issues arise with the introduction of new product names, logos and icons. Filing a trademark application with the U.S. Patent and Trademark Office can be an important step in claiming and protecting one’s rights in that mark.
Mobile payments providers operate in a highly regulated environment and must meet legal requirements and manage relationships with a wide range of parties, including consumers, merchants and employees. Potential litigation from any one of these parties may impair business operations and impose substantial and unforeseen costs on payments service providers who have not taken steps to prevent or mitigate litigation risks. In addition, regulatory agencies can bring enforcement actions. The following section identifies some litigation risks in the mobile payments context.

The regulations and case law governing disputes involving mobile payments providers is constantly evolving, and mobile payments providers face litigation risks from multiple sources. To mitigate litigation risk, mobile payments providers should identify risk areas relating to each of its business relationships and regulators; develop policies and procedures that comply with all applicable laws, including unfair, deceptive or abusive acts or practices case law and guidance; monitor complaints and analyze trends that may identify possible risk areas; focus on vendor management; and ensure they are adhering to accepted industry “best practices.”

**KEY POINTS**

**Litigation Risks**

- **Possible Claims.** In addition to claims arising from violations of federal laws, the possible claims against mobile payments providers also include: breach of contract, negligence, breach of fiduciary duty, invasion of privacy, violation of state unfair or deceptive acts or practices statutes, and violation of state security breach notification laws. Plaintiffs may recover actual damages, statutory damages under certain laws, punitive damages under certain common law claims, as well as attorney’s fees and costs.

- **Security Breach.** Mobile payments providers obtain and store large amounts of personal and financial data about parties to payments transactions and have legal responsibilities to protect that information. Security breaches expose mobile payments providers to reputational risk, as well as potential lawsuits by private plaintiffs (customers and credit card issuers), the FTC, and state attorneys general.

- **Privacy.** The use of mobile payments data for purposes other than processing transactions can present litigation risks for potential violations of privacy laws. These uses include: targeted advertising, location tracking, cookies, children’s data and collecting and/or selling personal information without the consumer’s knowledge or consent.

- **FCRA.** Under the Fair Credit Reporting Act (“FCRA”), there is litigation risk for entities that obtain consumer credit data without a permissible purpose. Mobile payments providers covered by the FCRA that do not comply with its legal requirements may be subject to civil penalties and class action lawsuits.
• **Trade Practices.** Under Section 5 of the Federal Trade Commission ("FTC") Act and Section 1031 of the Dodd-Frank Wall Street Reform and Consumer Protection Act, mobile payments providers may be subject to enforcement actions by the Consumer Financial Protection Bureau ("CFPB"), the federal banking agencies, the FTC and/or state attorneys general for engaging in unfair, deceptive or abusive acts or practices. Most state laws also provide consumers with private rights of action. This creates litigation risks that are complex and particularly difficult to manage, especially if mobile payments providers have to defend investigations and/or litigation by a combination of federal agencies, state agencies and/or private plaintiffs.

• **TCPA.** The Telephone Consumer Protection Act ("TCPA") regulates the delivery of telemarketing and non-marketing text messages sent to consumers. Mobile payments providers may be liable for potential TCPA violations, including the acts of third-party telemarketers, either expressly under the statute or under common law agency principles. Statutory damages of up to $1,500 per violation are available to consumers, and have led to an explosion of TCPA class action lawsuits.

• **Vendor Practices.** Mobile payments providers may be liable for the actions of their third-party vendors, as well as for claims brought against these vendors. Federal banking agencies, the CFPB, and the FTC have the authority to regulate services performed for a regulated financial institution. The CFPB, in particular, has brought numerous enforcement actions against regulated entities based on the acts of their vendors. Mobile payments providers and their vendors may be at risk of enforcement actions by these agencies.
Virtual Currencies and Other Emerging Payments

- **Payments and Virtual Currencies.** Consumer interest in adopting mobile payments is driven, in part, by the ease with which mobile payments allow consumers to engage in online transactions. For similar reasons, some consumers may choose to participate in online communities or networks that allow consumers to transact using virtual currencies, such as Bitcoin. The use of virtual currency has garnered substantial regulatory and law enforcement interest, and mobile payments providers who support the use of virtual currency should be aware of the complex web of state and federal laws that could apply, as well as the uncertainty surrounding whether such laws apply to transactions involving virtual currency.

**KEY POINTS**

**Virtual Currency Regulation**

- **BSA Applicability.** The Financial Crimes Enforcement Network ("FinCEN") has issued interpretive guidance to clarify the applicability of the Bank Secrecy Act ("BSA") and its implementing regulations to persons creating, obtaining, distributing, exchanging, accepting or transmitting virtual currencies. The guidance addresses "convertible" virtual currency (i.e., virtual currency that either has an equivalent value in real currency or acts as a substitute for real currency). The guidance defines "users," "administrators" and "exchangers" of convertible virtual currency, and explains which of these roles could be viewed as money services businesses ("MSBs") subject to regulation and enforcement under the BSA and FinCEN's implementing regulations. Among other requirements, MSBs must register with FinCEN, report suspicious activity and certain currency transactions, establish an effective anti-money laundering program, which includes verifying customer identification, and retain specified records.

- **State Licensing.** Like FinCEN, some states have looked into whether participants in virtual currency environments are engaged in money transmission. For example, the California Department of Financial Institutions ("DFI"), now the California Department of Business Oversight, issued a cease and desist letter to Bitcoin Foundation, a not-for-profit organization established to standardize, protect and promote the use and adoption of Bitcoin. The DFI stated in its cease and desist letter that Bitcoin Foundation "may be engaged in the business of money transmission without having obtained the license or proper authorization required by" California’s Money Transmission Act. The New York Department of Financial Services ("DFS") also has been active on this front, issuing an order stating that the DFS will consider applications for the establishment of virtual currency exchanges, issuing subpoenas to participants in the Bitcoin ecosystem, and holding public hearings on, among other things, the merits of a "Bitlicense." In the context of mobile payments, providers that facilitate the exchange of virtual currency and "real" currency via a mobile platform should consider whether they are subject to state licensing requirements.

- **Applicability of Consumer Protection Laws.** Federal regulators have yet to address the manner in which federal consumer financial protection requirements, such as the Consumer Financial Protection Bureau’s Regulation E, apply to transactions involving virtual currency.
Where mobile payments providers facilitate transactions in virtual currency, the extent to which consumer protections apply to virtual currency transactions remains unclear. For example, must a mobile payments provider facilitating transactions in virtual currency provide the disclosures or dispute and cancellation rights required for remittance transfers under Regulation E? In a virtual currency transaction, it may be impossible to ascertain whether the designated recipient is in a foreign country. The difficulty of determining the geographic location of a counterparty also creates challenges with regard to anti-money laundering reporting requirements.
1. This primer is for informational purposes only and does not constitute legal advice or create an attorney-client relationship. The information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome. Consult your own attorney for legal advice on the issues discussed in this primer. This primer may constitute attorney advertising.

To ensure compliance with the requirements imposed by the IRS, we inform you that any tax advice contained in this primer was not intended or written to be used, and cannot be used, for the purpose of (i) avoiding tax-related penalties under the Internal Revenue Code, or (ii) promoting, marketing, or recommending to another party any matters addressed herein.

© Morrison & Foerster LLP 2015