Money Transmitter Regulators Association

Exploring the New Frontiers of Mobile and Social Payments—Products, Players and Paradigms

Heidi Wicker
Schwartz & Ballen LLP
October 5, 2011
Overview

- Products--
  - What is a mobile or social payment?
  - Where are the new frontiers?

- Players & Paradigms
  - Who is staking a claim? Who has responsibility for what?

- Identifying Legal and Compliance Challenges

- Looking Towards the Horizon
  - Potential Regulatory Developments (?)
What are Mobile & Social Payments?

- Mobile payments:
  - Remote payments--May be initiated using:
    - SMS text messaging
    - Wireless internet on a mobile device
  - Proximity payments--May be initiated through:
    - Near Field Communications (NFC) chip on mobile device
    - “FOBs” or other access devices
    - Barcode technology displayed on mobile device
    - Card/other access device readers plugged into mobile device

- Social payments:
  - Prepaid, virtual “currency”
    - Usable within a defined, social networking environment
    - Dollar based/points based
  - “Daily deal” prepaid vouchers
How are they funded and used?

- **What are the Funding Options?**
  - Credit/debit cards
  - Prepaid cards
  - ACH
  - Stored value—open loop/closed loop

- **What Can Mobile and Social Payments Used For?**
  - P2B Payments—payment to a merchant for goods/services, acquired through mobile devices.
    - Online or in physical retail locations
    - Single merchant/multi-merchant
  - P2P Payments—money transfer to another person, not for payment of a good/service.
  - B2B Payments—payments by a business to suppliers
  - Bill Payment—utilities, etc.
  - Mobile banking
  - Rewards, coupons . . . And the list goes on . . .
How are Payments Initiated?

- **Application-generated barcode**
  - Application on device generates barcode, which is readable by merchants and represents payment for the item.
  - Purchaser may pay from a prepaid balance held by a third party, charged by a third party to a credit account, or debited from bank account.
  - E.g., recent Starbucks & Target gift card initiatives

- **Application/NFC Chip**
  - Purchaser or merchant, depending on the application, logs in to payment application on a smart phone
  - Selects payment device/card stored on multi-use NFC chip
  - Payment device/card info is read from the NFC chip by a reader at a merchant location
  - E.g., ISIS, Visa & Google mobile “wallet” initiatives
Starbucks Card Mobile App for iPhone
(Barcode Technology)

*Example: Barcode Technology displayed on mobile phone

Source: http://www.starbucks.com/coffeehouse/mobile-apps/starbucks-card-mobile
Google Wallet
(NFC Chip)

How it works

1. Look for these symbols at checkout.

2. Tap your phone on the reader.
   Your phone sends payment and, at some merchants, offers and loyalty information.

Source: http://www.google.com/wallet/how-it-works.html
**Tabbedout**
(a “fun” example)

Source: [http://www.tabbedout.com/sections/13/how-it-works/consumers/pay-your-tab](http://www.tabbedout.com/sections/13/how-it-works/consumers/pay-your-tab)
How are Payments Initiated?

- **Virtual Currency**
  - Merchant indicates it accepts the virtual “currency” of the social media interface.
  - Purchaser logs in to social network account.
  - Initiated through social network-hosted interface (social network may or may not be the merchant)
  - E.g., social/gaming networks, Bitcoin, Facebook Credits.

- **Plug-in/Swipe Devices**
  - Hardware provided by a third party that plugs into the merchant’s smartphone and is used in conjunction with an application; becomes a mobile POS device.
  - Can read magnetic stripe on payment cards. May also scan a barcode representing payment on a customer’s device.
  - E.g., Square, Verifone products
Facebook Credits
(Virtual Currency/Social Payments)

Step 1: Visit the game you want to buy credits for.

Step 2: Select method of payment (mobile phone option).

Step 3: Select number of credits you would like to buy.

Step 4: Enter your mobile number for payment. You will have to confirm payment through text messaging.

Source: http://mobilepaymenthelp.com/2011/07/22/mobile-payment-for-facebook-credits/
Square
(Plug-in/Swipe Devices)

Source: https://squareup.com/
Players and Paradigms—
Roles & Responsibilities

● Consumers/customers
  ● Provide authorization for payment credentials to be used to initiate payment to recipient/merchant
  ● May download payment applications, add payment information manually

● Banks (Card issuers, merchant acquirers, prepaid issuers)
  ● NFC--pushes bank-issued payment credentials to chip on customer’s phone
  ● Card payments--authenticates customer and authorizes payment
  ● Stored value--holds funds; nonbank entity may do recordkeeping
  ● Settles to recipient/merchant of payment, or may settle to a nonbank entity who settles to recipient/merchant
  ● Enter into agreement with payment service provider
Players and Paradigms—
Roles & Responsibilities

- Payment Card Brands/Networks—e.g., NACHA, Visa/MasterCard
  - Among other rules, implement liability/dispute resolution and customer protection rules, in compliance with banking laws
  - Issuing and acquiring banks, merchants and their service providers (e.g., processors) are required to comply with standards for the security of cardholder/customer information
    - PCI DSS (specific mobile device/application standards under development)
  - Help set the risk tolerance level for participants ➔ Limits what payment services can be provided to consumers.
  - Enforce rules against high risk participants ➔ Industry self-regulation.
  - Rules are applied to banks as a condition of participation in the network.
    - Banks required to implement the network rules through agreements with merchants and service providers.
    - Any processor/service provider acting on behalf of the bank and entering into agreements with merchants must also implement the network rules by agreement with merchants.
Players and Paradigms—
Roles & Responsibilities

● Carriers
  ● Provide wireless internet and phone capacity
  ● May bill customer’s payment transactions from third parties to phone bill (“carrier billing”)
  ● Joint venture (ISIS) developing a mobile wallet through which customer can store bank card payment info

● Technology/Mobile Service Providers
  ● May provide applications or permit developers to provide applications accessing customer payment info.
  ● May host certain payment, transaction or other information for customers in the “cloud.”
  ● May issue virtual currencies/stored value and/or partner with bank for assistance.
  ● May act as a payments processor.
Players and Paradigms—
Carriers & Technology/Mobile Service Providers, MSB Analysis

- May or may not be a money transmitter.
  - Law varies and depends on particular business structure.
  - Questions to be considered:
    - Which entity transmits payment data?
    - Which entity holds prepaid account balances?
    - Which entity does the recordkeeping and/or accounting?
    - Who does the entity act on behalf of?
      - Does the entity have an agreement with the customer for payment services?
      - Does the entity act on behalf of a regulated financial institution which, in turn, provides the payment services to and assumes the liability to customer?
      - Does the entity act on behalf of a merchant selling its own goods/services?

COMPLIANCE TIP→ Prior to entering into an agreement with a third party, consider requesting opinion of legal counsel that licensure is not required.
Legal/Compliance Challenges

- Unauthorized Transactions/Billing Errors/Chargebacks
  - Where an alternative payment mechanism is used, who is responsible? What regulatory regime applies? Who has authority to regulate nonbank participants?

  - As to carriers, jurisdictional issues to be considered.
    - Federal Communications Commission regulates carriers under interstate and int’l telephone law as “non telephone services”
    - State public utility regulations vary.

- As to nonbank entities → Consumer Financial Protection Bureau (CFPB)
  - Supervision authority over larger nonbank participants in, among others, money transmission and prepaid card industries
  - Rulemaking authority for EFTA/Regulation E, among other laws, transferred to CFPB
  - Can bring enforcement actions for unfair, deceptive, or abusive acts or practices or discrimination
  - Charged with operating a consumer complaints center, consumer education and research of consumer behavior
Legal/Compliance Challenges

- **Issues CFPB might address re: mobile/social payments:**
  - Consumer dispute rights
  - Disclosures
  - Revise definitions of who is subject to federal financial protection regulations

- Consumer groups, such as the Consumers Union\(^1\), have called for CFPB to:
  - Ensure consumers have the same mandatory protections against unauthorized transactions and billing errors with credit cards
  - Provide chargeback rights at the federal level for payments linked to bank debit/credit cards, prepaid cards and phone deposits.
  - Amend Regulation E to include a right to reverse charges disputed where the goods/services are not as delivered or agreed upon.

Legal/Compliance Challenges

- At the state level, consumer groups also have called for protection of consumers who make non-communications related mobile payments to prepaid phone deposits or phone bills.

- A related consideration for mobile payments is whether, for B2B payments, is the liability allocation under UCC 4A applies?
  - UCC 4A governs B2B wire transfers and ACH credit transfers.
  - Allocates liability based on whether set security procedures between bank and business are met.
  - NCCUSL Uniform Law Commission has not made any pronouncement as of yet as to applicability to mobile payments.
Legal/Compliance Challenges

- **What laws apply?** Depends on what data is being transmitted or maintained and the role of the party involved.
  - Laws/rules that may apply: Gramm-Leach-Bliley Act; State data security/data breach laws; Payment network rules

- **Who “owns” customer data which may be provided to enable the transactions, or arising from the transactions?**
  - When you have various parties involved—each may view the customer as their “own.”
  - May depend on what customer has authorized by agreement with the provider or its FI, and what the participants have agreed to among themselves.

- **Are there data use rights/limitations?**
  - May depend on what the customer has authorized, and what is prohibited by law (e.g., reuse limitations on account numbers under GLBA).
Who is responsible for protection of credentials, customer transaction and other information, at rest and as transmitted?
  - How to define the boundaries responsibility is being examined by the PCI Council, as well as the Federal Reserve and FCC.

COMPLIANCE TIPS

- Provide notice of privacy/data security practices in user agreements.
- Require affirmative consumer consent to changes in practices.
- Restrict by agreement what third parties, such as merchants, can do with customer data.
- Ensure technology is thoroughly tested in accordance with industry standards.
- Audit, or require audit report results to be periodically submitted, to ensure compliance.
- Prohibit “data passing” of customer data collected to a party which customer has not specifically authorized to receive the data for payments.
- Pass through these requirements to third parties with which you enter into agreements and monitor their ongoing compliance.
### Legal/Compliance Challenges

#### AML/KYC
- Who is responsible for conducting AML/KYC (CIP for banks) on customers/agents? And under what standards?
- Does new FinCEN prepaid access rule apply to all or part of transaction?
- Evaluation of customers and merchants at sign up and continual monitoring is key.

**COMPLIANCE TIPS**
- Ensure any partner is required by agreement to comply with and are educated in your AML/KYC standards.
- Consider requiring partners results of independent AML reviews/detailed description of AML controls, as appropriate based on their role.
Legal/Compliance Challenges

- **AML Compliance Tips, cont’d**
  - Ensure that you “know your merchant” if processing payments for merchants—look out for merchant “layering”

- **Handling of Customer Funds**
  - **COMPLIANCE TIPS**
    - Ensure any partner segregates corporate funds from customer funds.
    - Monitor partners’ solvency.
    - Include contractual right to request periodic financial reports/audits.
Looking Towards the Horizon—Potential Regulatory Developments?

- Developments To Watch in 2011:
  - FinCEN Prepaid Access Rules
  - Impact of Durbin(?)
  - Regulation E/Cross-border Remittance Rules
  - Enforcement actions
  - Federal Reserve Mobile Payments Working Group
  - Development of Industry Standards
    - PCI Council guidance
  - Federal and state legislation
Questions & Discussion