

**Mobile Banking/Mobile Payments 2012:
Hot Topics For Financial Institutions, Vendors and
Third-Party Payment Providers**

(IBAT TechMecca 2012)

Erin F. Fonté, Shareholder
Cox Smith Matthews Incorporated
January 23, 2012

Disclaimers

- The opinions expressed in this presentation are solely those of the presenter and do not necessarily reflect the opinions of Cox Smith Matthews Incorporated.
- This presentation is an educational tool that is general in nature and for purposes of illustration only. The materials in this presentation are not exhaustive, do not constitute legal advice and should not be considered a substitute for consulting with legal counsel. Cox Smith Matthews Incorporated does not have obligation to update the information contained in this presentation.

Introduction and Roadmap

- Jumping-off point: PAYMENTS – The new darling of VC's everywhere.

“Since the start of the economic crisis [in 2008], 239 financial services start-ups have raised almost **\$1.6 billion** in venture capital financing.”*



*(MoneyTree Report, PricewaterhouseCoopers and National Venture Capital Association.)

Introduction and Roadmap

- Federal Reserve Summary of “Meeting between Federal Reserve Staff and Representatives of ISIS (May 23, 2011)” (publicly available through Fed’s website)

“Representatives of ISIS met with Federal Reserve staff to provide an overview of the ISIS payment platform and discussed the Board’s proposed prohibitions on network exclusivity and routing restrictions as part of the proposed rule to implement Section 1075 of the Dodd-Frank Act. Representatives of ISIS provided an **overview** of the payments platform and **making payments** at the point-of-sale using the platform, the **roles of the various participants** in the platform, and **privacy** and **security** features of the platform.”

Introduction and Roadmap (cont'd)

- Mobile growth; mobile banking and payments
- “Payments 101” (condensed)
- Key Regulations Regarding Mobile Payments
- Various Scenarios and Related Issues
 - FIs using 3rd parties to provide “white label services” (platforms re-branded as bank’s own product)
 - FIs (a) banking 3rd party payments provider (“acquiring”) and/or (b) banking 3rd party to be “issuer” side for mobile payments (i.e. end-user customer sub-accounts)
 - Merchants considering 3rd party technology and/or services for accepting and making payments
- Odds and Ends

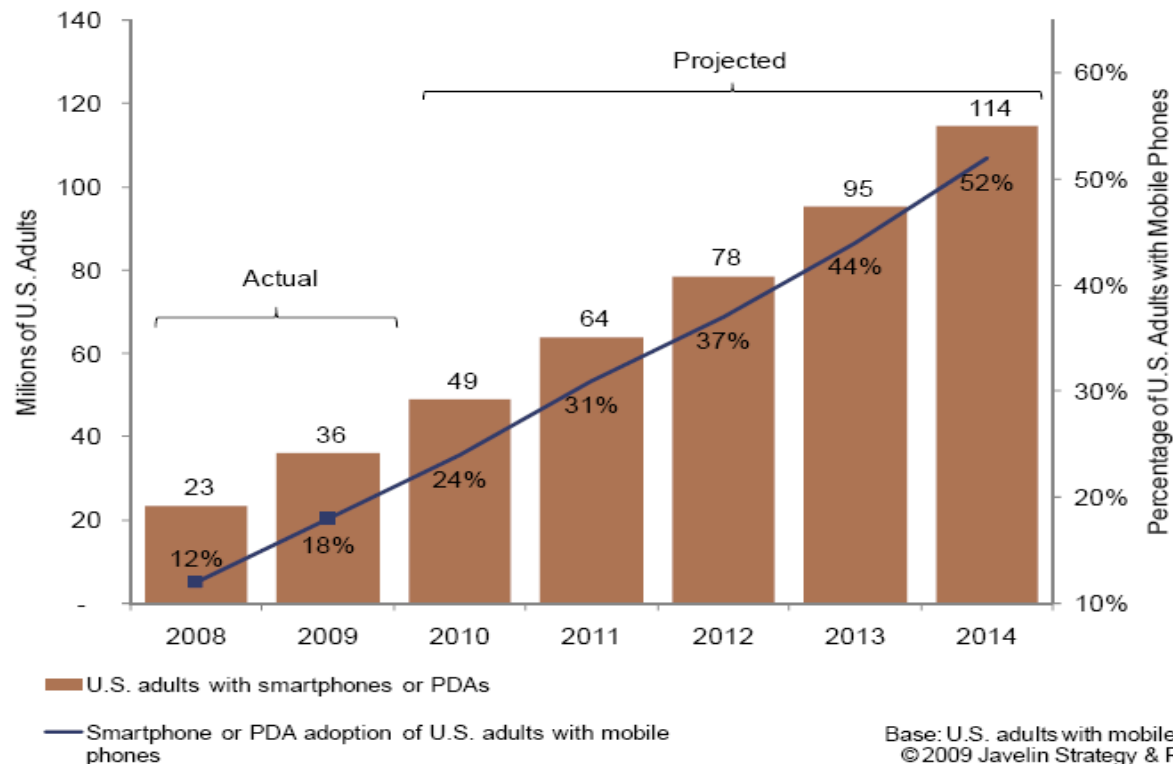
Mobile Growth

- Predictions that in first half of 2012 the 6 billion mobile subscribers globally mark will be reached
- Mobile devices have now far outpaced the number of personal computers
- In the U.S., more text messages are now sent than voice calls via mobile

Mobile Adoption

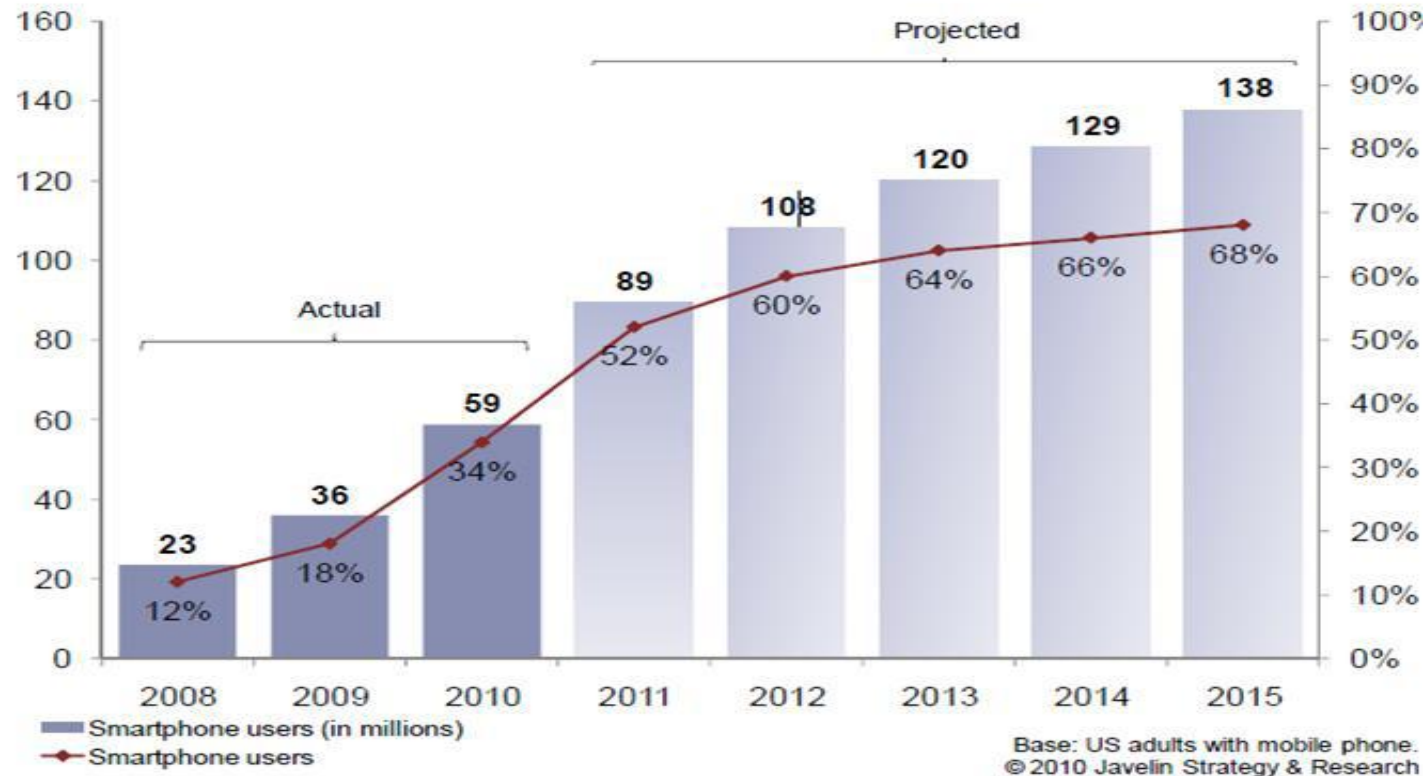
Javelin Five-Year Forecast for Smartphone Share

Figure 7: Number and Percentage of U.S. Adults Owning Smartphones



Mobile Adoption (cont'd)

Figure 5: Javelin's Five-Year Forecast of Adult Smartphone Users, 2008–2015



Mobile Banking: Expanding Customer Options

■ Mobile Banking

- FI customer accessing (and effecting transactions to) an account held at the FI through a mobile device

■ Mobile Payments

- Mobile payments are payment transactions between two parties initiated by means of a mobile device (THIS IS BANKING DISRUPTION)
- Mobile payments occur in two principal forms:
 - *Proximity Payments* – where technology embedded in/displayed on the payor's mobile device interfaces with the payee's point-of-sale equipment to initiate payment
 - *Remote Payments* – where the payor uses mobile device capabilities to initiate payment to the payee without regard to proximity to the payee/point-of-sale

Mobile Banking: Expanding Customer Options

- More than 1 million customers enrolled in Text Banking
- More than 6 million Mobile Banking customers
- More than 29 million active online banking users and 200 million log-ins per month
- More than 15 million customers who pay more than \$230 billion in bills electronically each year
- Stakeholders/Payments Ecosystem:
 - Traditional Players: Banks, Merchants, Payment Brands
 - Mobile Players: Mobile Device Manufacturers, Wireless Carriers, App Developers

“Payments 101” Condensed



- **“Payment”**: transfer of money or wealth or value from one party to another
- FIs: accept, collect, and process payments; participate in clearing and settlement systems
- Non-FI Third Parties: increasingly involved and can introduce new risks
- New payment methods and access channels = rapid and convenient transmission of payment information among system participants
- But can also enable propagation of **fraud, money laundering, and traditional banking operational disruption**

“Payments 101” Condensed (cont’d)

■ 5 – And ONLY 5 – Payment Channels (“payment rails”)

- Cash
- Check (paper; Check 21 “substitute check”)
- ACH (closed-system model; includes paper checks converted to ACH)
- Credit/debit/stored value cards (open-loop cards)
- Wire transfers



Payment Types/Channels – New/Emerging

- **Electronification of checks**
 - Substitute Checks and Images (Check 21)
 - E-Checks through ACH networks (ARC, BOC, POP)
- **Newer/Emerging Technologies**
 - Web/online payment (banks and non-banks)
 - Contactless cards/devices
 - Mobile (smart phones, mobile wallet (Google Wallet, ISIS, Starbuck's payment app))
 - Second Life: virtual money, virtual banks, real payments
 - BitCoin? If criminals and drug dealers love it, it may not be around long...



“Payments 101” Condensed (cont’d)

- The 5 “rails” developed independently of each other.
- Thus, separate legal/rule structures exists for each payment type, and legal rights and remedies vary depending upon the “rails” the payment travels on
- For example, ACH transactions
 - Electronic Funds Transfers Affecting Consumer Accounts
 - Electronic Funds Transfer Act (EFTA) and Regulation E – NOT APPLICABLE TO COMMERCIAL TRANSFERS
 - NACHA and ACH Operator Rules – e.g. 60 day window for consumer to dispute ACH payment
 - UCC Article 4A in certain circumstances outside scope of NACHA/ACH rules

Regulatory Issues in Mobile Payments

- To date, mobile payments initiatives in U.S. have largely leveraged existing payment and funds transfer methods/rails
 - The regulatory regime applicable to existing methods and models most likely governs mobile payments analogues
- Regulatory picture becomes less clear in certain operating models that may become prevalent in the future
 - Mobile Network Operator model where customer purchases of third party goods/services are reflected on the customer's wireless bill
- Increased involvement of non-banks may pose enhanced regulatory and supervisory challenges
 - Consumer Financial Protection Bureau (Card Market division)
 - Newly formed "Interagency Task Force" on 3rd party payment services providers (FTC, DOJ, FBI, FinCen, OCC and FDIC)

Regulatory Landscape – Mobile

- Look to regulations that apply in traditional payments landscape (because mobile is touching at least one, if not multiple, of the 5 existing rails)
- What regulations apply to the underlying bank products? (*HINT*: Odds are they still apply in the mobile payments space)
- How do we present required disclosures?
- “Shared responsibilities” for compliance – goes into the agreements between parties
- Why is regulatory important? Horrible scenario to invest time, money/venture capital money in launching a product that a regulator can shut down with one unfavorable interpretation

Electronic Funds Transfer Act/ Regulation E

- Generally applies to “any person that directly or indirectly holds an account belonging to a consumer, or that issues an access device and agrees with a consumer to provide electronic fund transfer services”
 - “account” means a consumer asset account
 - “access device” means “a card, code, or other means of access to a consumer’s account . . . that may be used by the consumer to initiate electronic fund transfers”
- A mobile device that can be used to initiate electronic fund transfers from a consumer asset account (e.g., a DDA) is most likely an access device for EFTA/Regulation E purposes and the issuer of the mobile device (and the holder of the account, if different) is most likely subject to the EFTA/Regulation E

Electronic Funds Transfer Act/ Regulation E (cont'd)

- AND Fed has shown it is not ignorant of “devices with a chip or other embedded mechanism that links the device to stored funds, such as a mobile phone” (new comment 20a-1 to new Regulation E provisions that implemented the CARD Act’s gift card fee and expiration date prohibitions)
- Fed has been willing to re-visit what Reg E applies to (e.g. payroll cards – first it didn’t apply, now it does)
- *HINT*: PayPal assumes it is subject to Reg E, so you might want to as well; OR at least do the analysis on the front end
- Fed so far has not announced its position about whether wireless carriers are subject to most Reg E requirements as “service providers” under Section 205.14

Truth In Lending Act/Regulation Z

- Applies in relevant part to any person that issues a credit card and who regularly extends credit to consumers primarily for personal, family or household purposes
 - A “credit card” is “any card, plate, coupon book, or other single credit device that may be used from time to time to obtain credit.”
- Mobile device linked to a credit card = subject to TILA/Reg Z, but bank issuing CC is issuing credit, so Bank is subject to TILA/Reg Z
- Mobile Network Operator that allows charges to wireless bill = probably not subject to TILA/Reg Z, but separate state and federal “truth in billing” laws will apply
- Also, payment service providers (like PayPal) typically not subject to TILA/Reg Z
- Consumers generally look to issuing banks for TILA/Reg Z compliance and disclosures

USA Patriot Act/ Bank Secrecy Act/ AML Requirements

- Financial institutions, including money services businesses (MSBs), are subject to various requirements designed to detect and prevent money laundering and terrorist financing activities
 - Banks are expressly covered by BSA requirements
 - Many mobile payments service providers are subject to BSA compliance obligations as money transmitters (i.e., MSBs)
 - Mobile network operators, depending on their role in facilitating funds transfers, may also be subject to regulation as MSBs if they satisfy the definition of a money transmitter or operator of a credit card system
- Know your customer/Customer Identification at account opening
- Policies and procedures to monitor and detect money laundering
- Office of Foreign Asset Control (“OFAC”) scrubs
- Mobile payments provide unique challenge to AML programs; button this issue up tight, or regulators will step in and make you

USA Patriot Act/ Bank Secrecy Act/ AML Requirements (cont'd)

- FinCEN's final rule on "prepaid access" - characterizing all "providers of prepaid access" as MSBs will pull additional non-bank participants in pre-funding mobile payments schemes under federal supervision for AML compliance (also duties for "sellers" of prepaid access as agents of "providers of prepaid access")
- FinCEN has defined "prepaid access" very broadly, to include any: "electronic device or vehicle, such as a card, plate, code, number, electronic serial number, mobile identification number, personal identification number, or other instrument that provides a portal to funds or the value of funds that have been paid in advance and can be retrievable and transferable at some point in the future."

Gramm-Leach-Bliley Act

- Applies to “financial institutions,” as broadly defined
 - Privacy Rule – requires FI to disclose to customer its policies regarding disclosure of customer’s nonpublic information with affiliates and non-affiliates
 - Safeguards Rule – requires FI to develop standards to protect customer information
- Applicability of GLBA to non-bank mobile payments provider will vary with the model, but should apply to mobile payments entities in parallel to its applicability to providers involved in more traditional payment channels
- Banks and mobile service providers will be dealing with many 3rd parties (mobile network operators, wireless carriers, app developers) and should consider placing privacy provisions in 3rd party vendor contracts and harmonizing their own privacy policies – e.g. 3rd party marketing

Uniform Commercial Code Article 4A

- Governs B2B wires and Automated Clearing House transactions – except it contains giant “variation by agreement” loophole in 4A-501
- Separate National Automated Clearing House (NACHA) and regional clearing house association rules (private contract) - NACHA rules are 200+ pages long and anyone generating ACH debits/credits must abide by them
- 4A excludes anything covered by Reg E (and vice versa)
- 4A sets up different liability scheme than Reg E (and recent cases interpreting this)
- Wires via mobile phone? Governed by 4A?

State Money Transmitter/ Money Services Laws

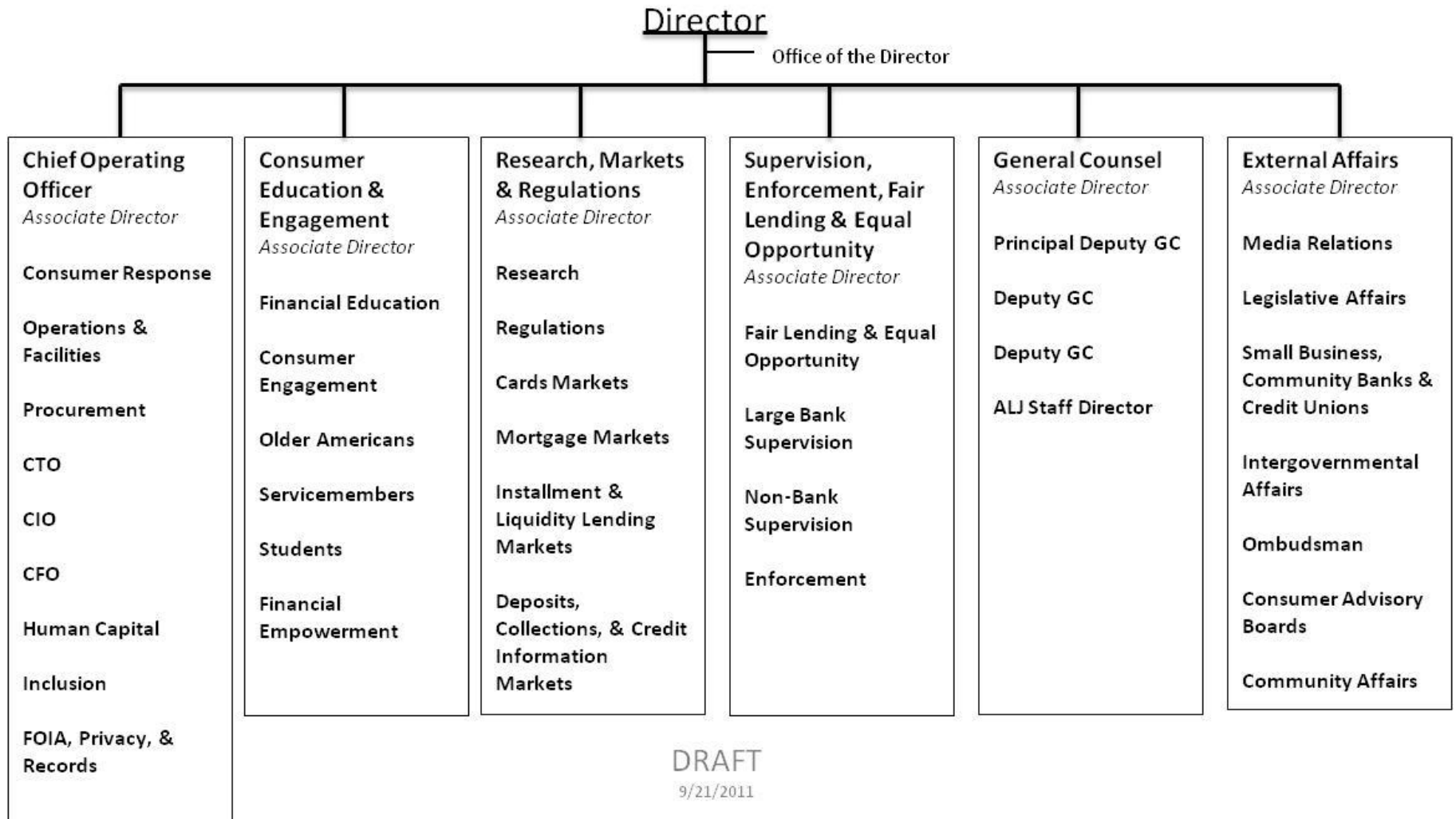
- Govern the activity of non-depository money service (funds transfer) providers like money transmitters, check cashers and currency dealers
- E.g. Minnesota law definition of “money transmission”
 - Selling or issuing payment instruments or engaging in the business of receiving money for transmission or transmitting money within the U.S. or to locations abroad by any and all means, including but not limited to payment instrument, wire, facsimile or electronic transfer.
 - PayPal, for one, found out the hard way these state laws have teeth; it now has licenses in 42 U.S. states and territories, and has obtained opinions it does not have to be licensed in 7 additional states (each state is different)
- Except to the extent that a bank agent exemption may apply, mobile payments service providers and mobile network operators responsible for funds transfers (including P2P transfers and prepaid funding models) may be subject to state MSB/ money transmitter licensure
- Criticized as a barrier to entry, and state regulators say “**exactly**”

Dodd-Frank Act

- Title X - Consumer Financial Protection Act and the creation of the Consumer Financial Protection Bureau with authority to regulate non-bank providers of consumer financial products and services
- “Financial Products” include:
 - Extending credit
 - Issuing stored value or payment instruments
 - **“providing payments or other financial data processing products . . . including payments made through an online banking system or mobile telecommunications network”**
 - Durbin Amendment restrictions on exclusive network arrangements will likely impact all participants in the evolving mobile payments marketplace
 - New coverage of cross-border remittance transfers under the EFTA/Regulation E will impact all mobile initiated remittances to foreign receivers

Dodd-Frank Act (cont'd)

- CFPB: Richard Cordray was appointed head of the bureau in early January 2012 as an interim appointment by President Obama
- CFPB up, running and fully operational with all rulemaking authority
- CFPB has already launched its “Nonbank Supervision Program”
- CFPB Website: www.consumerfinance.gov
 - “Submit a mortgage complaint”
 - “Submit a credit card complaint”
 - “Sign up and tell your story”
- Cordray Speech at Brookings Institution (1/5/12)
 - Q: So do you think there is a role for altering the design of products as opposed to just making consumers better informed?
 - Cordray: I think that consumers need to be better informed. There are some practices that occurred in the market that are unacceptable and need to be fixed and we will deal with those as they arise.



Supplemental Guidance on Internet Banking Authentication (FFIEC) – June 28, 2011

- FFIEC Authentication Supplemental Guidance
 - Supplement to “Authentication in an Internet Banking Environment” (issued in 2005, supplement 6/28/11)
 - Effective January 1, 2012
 - **FFIEC Authentication**
 - Supplement includes changes/additional guidance for:
 - (1) risk assessments
 - (2) authentication for high-risk transactions
 - (3) layered security programs (not multi-factor, but different controls at different stages)
 - (4) effectiveness of certain authentication techniques
 - (5) customer education and awareness (esp. commercial customers)

FI “White Label” Services

- FIs use 3rd parties to provide products, apps, platforms that are re-branded as the bank’s own product – i.e. mobile banking app, personal financial management
- Regulatory Burden – most definitely on bank BUT a good 3rd party vendor seeking to provide services to FI will understand when FI requires a fix or new component for regulatory/compliance purposes
- 3rd party must also agree to abide by regulations where FIs required to obtain such promised from vendors
- Also, if ACH rails or debit/credit card rails are used, must also comply with NACHA Rules and credit card network association rules for vendors, etc. (And PCI-DSS where CC/debit card information used).
- FI standard 3rd party vendor due diligence package: SAS70/SSAE 16 audit

FI “White Label” Services

- Vendor: Can I show a potential FI client that I passed the Federal Financial Institutions Examination Counsel exam?
 - NO. A third party servicer (“TSP”) is in no way, shape or form authorized to make any reference whatsoever – on its website, in marketing materials, during sales calls, etc.- to the fact that it successfully passed an FFIEC exam (from FFIEC itself)
- Vendors need to be willing to work with FI customers based on what FIs need to meet regulatory and examiner requirements
 - But difficult for FI to really convey, for example, when need for change comes out of a regulatory exam, but FI is forbidden by its regulator from disclosing that contents/reports/information from exam are giving rise to the requested change (see 12 C.F.R. 309.6 (FDIC); 12 C.F.R. 261.20-23 (Fed); 12 C.F.R. 4.32-38 (OCC); and 12 C.F.R. 792.11, 792.30-32 (NCUE))
 - “Dear CFPB, Change This!!”

FI “White Label” Services (cont’d)

- Data security/customer information duties and obligations – on behalf of both FI and vendor; typical split of liability is if breach occurs while data in a party’s control, that party is responsible for dealing with it
- Vendor duty to notify FI of suspected or actual breaches and duty to aid in investigation
- Vendor to turn over financials and other info to FI (financial stability, etc.) on an ongoing basis – part of vendor due diligence
- Cooperation in customer loss issues – Reg E compliance by FI, etc.
- Dispute resolution mechanisms for settling disputed transactions or charges
- Requiring vendor to have cyberliability coverage?

FI Banking A 3rd Party Payments Provider

- Here the main issue turns to due diligence of the 3rd Party Payments Provider
- Debit and CC card network association rules (typically acquiring rules if FI is acting as the 3rd parties acquiring FI)
- NACHA Third Party Sender Rules and Requirements
- Due Diligence (and mind this new task force focused on the fact that FIs must be extremely diligent before opening accounts for “processors”)
- Issues similar to business customers with treasury management functions: credit underwriting; prefunding requirements; reserve accounts for disputes and chargebacks
- Regulatory Burden – both on FI (and NACHA and card network compliance) and on 3rd Party payments provider for its customers

FI “Banking” A 3rd Party Payments Provider and Acting in “Issuing” or “Acquiring” Role

- FIs partnering with “distributors” or other companies to provide an “issuing” or “acquiring” role with regard to CC/debit card products
- Or acting as ODFI to 3rd parties customers for payments
- Account structure issues (end-customer funds custodial accounts vs. company operating accounts vs. settlement accounts)
- 3rd party often has frontline end-customer service and disclosure obligations, but FI must oversee because FI is the one who will get cited in an exam for non-compliance
- Same for CC/debits card association rules, and NACHA rules
- Who owns the “end customer” data and can walk away with it.
- KYC/CIP – distributor/3rd party must conduct in accordance to what FI demands.

FI “Banking” A 3rd Party Payments Provider and Acting in “Issuing” or “Acquiring” Role

- FIs sponsoring 3rd parties or distributors into CC/debit card networks, NACHA, etc.
- FI approval over 3rd party/distributor “subagents”
- Compensation to parties involved, and reconciliation procedures
- Same issues regarding fraud and transaction disputes – reserve account, chargebacks, etc.
- Liability for fraud loss
- Termination and wind-down provisions
- Security program for end-user customer data, and who has responsibilities for breach, etc.
- Regulatory Burden – arguably can be equally on both FI and 3rd party/distributor for certain regulations

FI “Banking” A 3rd Party Payments Provider and Acting in “Issuing” or “Acquiring” Role

- FI review and approval of end-customer agreements and disclosures
- End-customer intake, KYC/CIP and approval process (especially for merchants)
- IF debit/CC, then FI must also be a party to any separate 3rd party processor agreement
- IP/Use of Marks – also governed for debit/CC by card network association rules
- All parties (FI, 3rd party/distributor, and any distributor sub-agents) must comply with all applicable rules and regulations
- Exclusivity issues – this can get a bit tricky, especially as new technologies develop

FI “Banking” A 3rd Party Payments Provider and Acting in “Issuing” or “Acquiring” Role

- Vendors need to be willing to work with FI customers based on what FIs need to meet regulatory and examiner requirements
 - But difficult for FI to really convey, for example, when need for change comes out of a regulatory exam, but FI is forbidden by its regulator from disclosing that contents/reports/information from exam are giving rise to the requested change (see 12 C.F.R. 309.6 (FDIC); 12 C.F.R. 261.20-23 (Fed); 12 C.F.R. 4.32-38 (OCC); and 12 C.F.R. 792.11, 792.30-32 (NCUE))
 - Real life example
 - Need this to be changed – ridiculous to prohibit an FI from telling its partner company why something needs to be changed due to exam finding

Merchant/3rd Party Agreements For Mobile Payments Services

- Does the mobile payment service provider (“MPSP”) have the proper processing capabilities (either in-house or via 3rd party processor) and do all parties have proper sponsorship into CC/debit networks, and other
- Clear dispute resolution procedures for disputed transactions and charges
- Must merchant put up reserve account, and if so, how is the amount calculated?
- Also, in event of a dispute, and there is no separate reserve account is the entire merchant account frozen while dispute is investigated?
- MPSP should represent and warrant that it complies with all applicable laws, rules and regulations
- Data security (PCI-DSS) and data security breach issues
- Clear and understandable merchant pricing structure

Merchant/3rd Party Agreements For Mobile Payments Services

- Financials and performance of MPSP (stability, ability to withstand problems)
- Security and authentication – how does the MPSP make sure the transactions occurring over its network are legitimate?
- Fraud prevention – what does the MPSP do?
- Merchant question – does the MPSP work with my physical POS and internet sales systems?
- One single payments providers, or hybrid?
- What can the merchant do in a “system down” scenario?
- Read the Merchant Agreement in detail, and don't be afraid to ask hard questions
- Ask for representative clients who already use the payment system

Odds and Ends

- **Authentication, authentication, authentication** – holy grail of remote payments, including mobile payments – look to FFIEC guidance on this
- **Geolocation Issues** – permission, permission, permission, and looking at voluntary Mobile Marketing Association “Mobile Application Privacy Framework Policy” (and watch FTC regulatory action on geolocation issues)
- **Geolocation Ad targeting** – (1) permission to use current geolocation info, and (2) prior, express written consent to send 3rd party ads to mobile phones (FCC Telephone Consumer Protection Act)
- **Visa/MC** – using CC transaction data to target web (and mobile) ads
 - So, so many privacy concerns; also whether issuing banks would all of the sudden be violating any GLBA model privacy notice statements that they do not share info for 3rd parties to market products and services

Odds and Ends

- **Authentication, authentication, authentication** – holy grail of remote payments, including mobile payments – look to FFIEC guidance on this
- **Geolocation Issues** – permission, permission, permission, and looking at voluntary Mobile Marketing Association “Mobile Application Privacy Framework Policy” (and watch FTC regulatory action on geolocation issues)
- **Geolocation Ad targeting** – (1) permission to use current geolocation info, and (2) prior, express written consent to send 3rd party ads to mobile phones (FCC Telephone Consumer Protection Act)
- **Visa/MC** – using CC transaction data to target web (and mobile) ads
 - So, so many privacy concerns; also whether issuing banks would all of the sudden be violating any GLBA model privacy notice statements that they do not share info for 3rd parties to market products and services

Odds and Ends (cont'd)

- Mobile as part of behavioral advertising 2.0, “predictive analytics” and merchant-funded rewards programs
 - Combining data from transaction history, social media activity/comments, and location to deliver ads for items you just began to think about buying
 - Getting merchants to help pay for loyalty and rewards programs where FI can show merchant’s revenue increased as a direct result of the FI program
 - Getting loyalty and reward program members to “tweet up” the merchant’s products or services to get even more points
- **Business Method Patent: Mobile Payment App**
- *Maxim Integrated Products Inc. v. Starbucks Corp.* Case 4:12-cv-00005-RAS (U.S. District Court, E.D. Texas (Sherman Division) (1/6/12)
- **Maxim filed same patent claims against Starbuck’s (retail), CapitalOne and Bank of the West (banking/FI) and Expedia (travel & leisure) alleging BMP infringement of mobile payment app**

QUESTIONS?

Erin F. Fonté, CIPP

Shareholder

Banking and Financial Institutions/
Privacy and Data Security

Cox Smith Matthews Incorporated
111 Congress Avenue, Suite 2800
Austin, Texas 78701
Direct: 512-703-6318
efonte@coxsmith.com



@PaymentsLawyer

LinkedIn  Link me in: Erin Fonte