

# EVOLVING MOBILE LANDSCAPE CHALLENGES AND OPPORTUNITIES

Technology, Compliance and Risk Management Forum

NY Bankers Association

June 7, 2012

Marianne Crowe

VP, Payment Strategies

Federal Reserve Bank of Boston

*Disclaimer: The views expressed in this presentation are those of the presenter and do not necessarily reflect the views of the Federal Reserve Bank of Boston or the Federal Reserve System*

# Agenda

- U.S. Mobile Payment Landscape
- Mobile Payment Opportunities
- Security
- Regulatory Landscape
- Mobile Payment Industry Initiatives
- Conclusions

# Mobile Banking & Payment Terms

- **Mobile Banking**
  - Use of mobile device to connect to an FI to view account or credit card balances, transfer funds between accounts, pay bills, receive account alerts, locate ATMs
- **Mobile Payment**
  - Use of mobile device to pay at POS or internet for goods, services or digital content, transit, P2P. Payment initiated via SMS, mobile internet, downloadable app, contactless NFC chip, barcode or cloud technology
- **NFC (near field communication)**
  - Communication protocol that enables contactless transactions, data exchange, and wireless connections between two devices (e.g. mobile phone and merchant terminal) in close proximity. NFC chip embedded in mobile phone, on SIM card, or on MicroSD chip.
  - Wave/tap phone at POS terminal to pay

# Mobile Banking & Payment Terms

- **Secure Element**
  - Encrypted, tamper-proof chip in mobile phone where payment credentials, application code, and financial data are stored and managed and where execution of payment application occurs
- **Mobile Wallet**
  - Software application loaded on to a mobile phone that enables multiple payment credentials and value-added services, such as bank and credit or debit card accounts, prepaid accounts, transit tickets, coupons, gifting, and loyalty to be securely accessed and managed to initiate mobile payments.
- **Cloud Wallet**
  - Mobile payment credentials and account information hosted on remotely located network servers – stored remotely in ‘the cloud.’ Payment credentials accessible via mobile phone app, mobile phone number and PIN, or a physical card
  - Uses virtual token to initiate ‘secure’ transaction
  - Consumers and merchants download apps to use cloud for mobile payments

# Trends in U.S. Mobile Payments Ecosystem

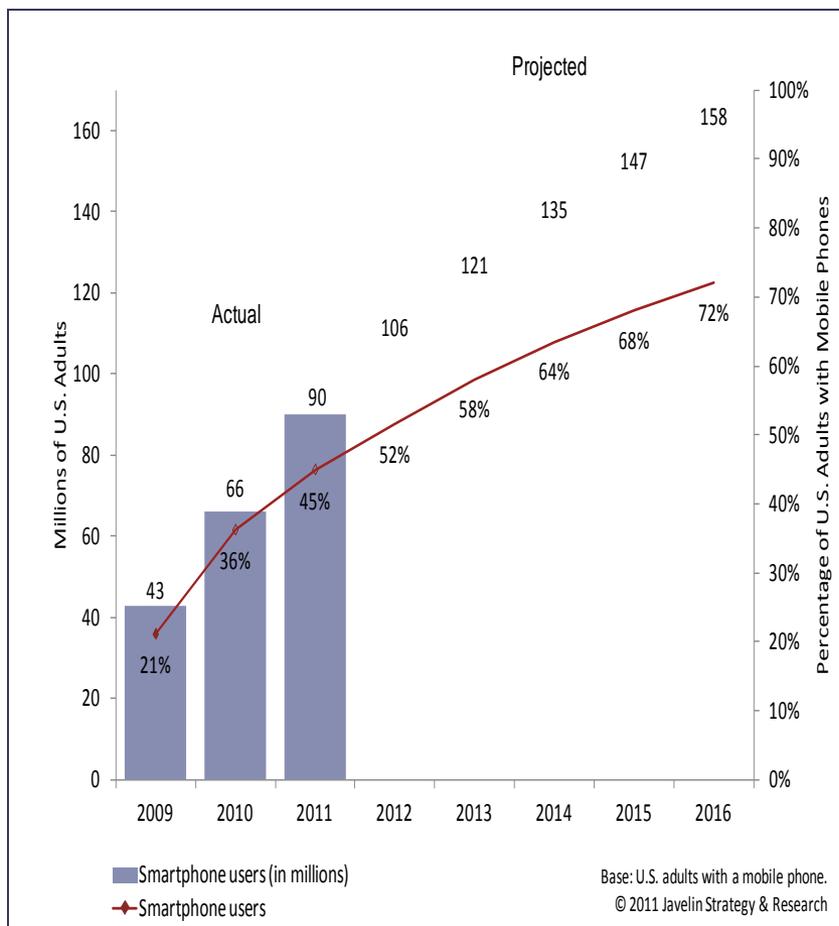
- Consumers making more mobile payments
  - PayPal mobile transactions increased 500% in 2011 over 2010
  - Google mobile shopping searches increased 220% in 2011 over 2010
- Mobile internet and remote purchases (m-commerce) still small, but increasing as more consumers buy smartphones and use more apps, incited by m-coupons, discounts and rewards
- Convergence of online, mobile and POS channels creating opportunity to use NFC and other mobile technologies
- Mobile wallet developments
- Visa/MasterCard mandate for EMV/Chip+PIN in U.S.
- Non-banks (Google, PayPal, Apple, Square, carrier billers) entering payment system
- Cloud emerging as another alternative for mobile payments

# Smartphone Adoption

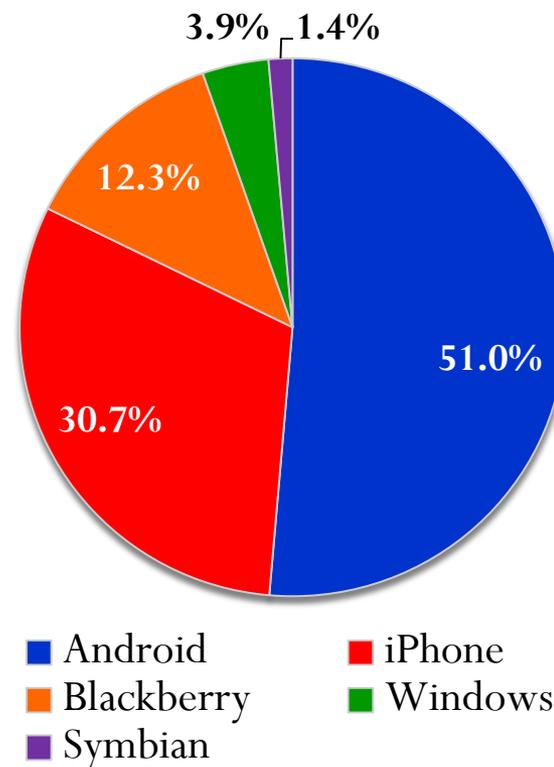
Smart phone adoption is a key driver.

- Can't go far in US with mobile payments without smart phone; Can't download apps, access web
- Can't do contactless payments (either NFC or barcode) at POS; Can't receive coupons, discounts, use LBS

## U.S. Adult Smartphone Adoption, 2009-2016



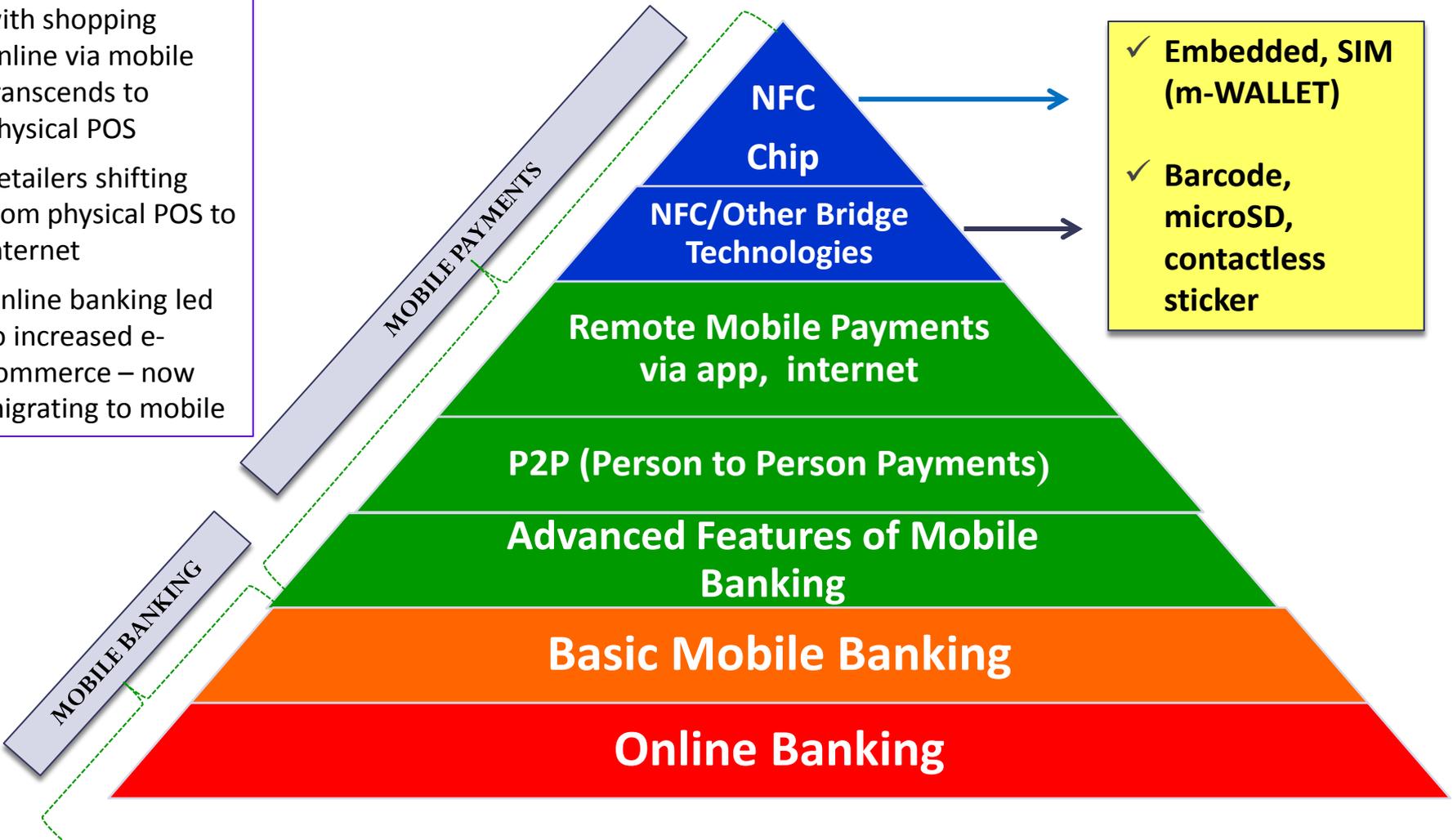
## U.S. Smartphone Market Share\* 1Q 2012



\*By operating systems  
Source: comScore, May 2012

# Evolution of U.S. Mobile Banking and Payments

- Customer comfort with shopping online via mobile transcends to physical POS
- Retailers shifting from physical POS to internet
- Online banking led to increased e-commerce – now migrating to mobile



# Mobile Remote Deposit Capture

- Mobile app uses camera to capture and transmit check image to FI for deposit, usually immediate availability
- Banks and non-banks offer to consumers and small businesses with low check volumes from remote locations
  - USAA, Chase, USB, PNC, Charles Schwab, Fiserv, PayPal
- Reduces bank and customer paper handling cost
- Growing in popularity – 38% of smartphone users want m-RDC (*Javelin, March 2011*)



## Fraud Controls

- Multi-factor authentication
- Secure (encrypted) transmission
- Limit on daily customer deposit amounts
- KYC, customer due diligence
- Monitor frequency of use
- Detection of duplicates, double-posting



# Bank-centric Mobile P2P Payments Evolving

- P2P electronifies personal checks or cash used for informal payments
- Small dollar money transfers via ACH less costly than wire
- Sender is bank customer
- Different models exist
  - Bank/card network partnerships – MC MoneySend, Amex Serve, Fiserv PopMoney (ZashPay)
  - Bank-owned – ClearXchange (Bank of America, Wells Fargo, Chase)
  - Non-bank – PayPal, Obopay

The screenshot shows the POPmoney mobile app interface. At the top, the status bar displays 'AT&T', signal strength, Wi-Fi, and the time '10:50 AM'. The app header features the 'POPmoney' logo in blue and green. Below the header, the text 'Pay Other People' is displayed in orange. The login form includes an 'Email:' field with the text 'charlietest@cashedge.com', a 'Password:' field with masked characters, and a 'Save Email:' toggle switch set to 'ON'. A large green 'Log in' button is positioned at the bottom of the form.

## Possible concerns

- More cross-border remittances
- Money laundering
- Need for more KYC

# Mobile Payment Opportunities

---



facebook



eBillme™  
MY BANK MY WAY



amazonpayments™



verizon

Google™  
Checkout

PayPal®



T-Mobile®

bobopay™



Zash pay™

MasterCard®  
MoneySend™

The NEW Payment  
Landscape: No Longer  
Just "Green and White"

intuit.



boku PAY BY MOBILE™

clearXchange™

ZONG®

PAYware Mobile  
Accept card payments anywhere.

Billeo.

BillMeLater™  
The Shopping Express Lane

mazooma.

Google wallet



twitpay

WESTERN UNION  
MONEY TRANSFER

Acculynk



my2check  
eCheck Processing for the 21<sup>st</sup> Century

CASH EDGE



Rialto Pay™

SAFETY PAY™  
The Safe Internet Payment Solution

Microsoft®

# Mobile Payment Opportunities

	Remote	Proximity
Platform	<ul style="list-style-type: none"> <li>• SMS text</li> <li>• WAP browser</li> <li>• Downloadable application</li> <li>• Direct Carrier Billing</li> <li>• Cloud</li> </ul>	<ul style="list-style-type: none"> <li>• NFC Contactless chip embedded in mobile phone, SIM card, or micro SD card</li> <li>• 2-D Barcode</li> <li>• Cloud</li> </ul>
Services	<ul style="list-style-type: none"> <li>• Remittances, P2P</li> <li>• Charitable donations</li> <li>• Ticketing (airline, movie, event, parking)</li> <li>• Internet purchases, digital content</li> <li>• Rewards, coupons</li> <li>• Marketing &amp; location based services</li> <li>• Support Financial Inclusion</li> </ul>	<ul style="list-style-type: none"> <li>• Retail POS purchases</li> <li>• QSR, convenience, drug store</li> <li>• Public transit, taxis, parking</li> <li>• Vending</li> <li>• Rewards, coupons</li> <li>• Marketing &amp; location based services</li> <li>• Support Financial Inclusion</li> </ul>

# 2D (QR) Barcode

- Download mobile app to access and read barcode
- Merchant driven, gets mobile payment solution to consumers more quickly
- Risk of infected QR code directing consumer to malicious website or app

## Starbucks (1-2011)

- Closed-loop prepaid account
- 9,000 locations U.S., Canada, UK
- Reload funds, track rewards
- 4.2M+ mobile transactions to date



## LevelUp

- 150,000 users
- 2,500 merchant partners
- 10 major cities
- Loyalty program
- Location-based offers and services
- PIN-lock QR code and phone





# NFC Wallets



- NFC chip embedded in mobile wallet
- Launched September 2011
- Limited to one mobile carrier - Sprint - and Citibank MasterCard on Samsung Nexus S 4G
- 10 more Sprint Android phones in 2012
- Google virtual prepaid account
- 30 merchants, including transit
- Coupons, merchant deals, loyalty programs
- NFC SIM card model
- AT&T, Verizon, T-mobile
- Chase, Capital One, Barclaycard
- Discover, Visa, MC, AMEX
- Summer 2012 trial
- Austin, TX and SLC, including UTAH Transit



# PayPal Wallet in the Cloud

- 103+ million active accounts (2012); *9M merchants*
- 8M mobile customers with daily purchases of \$10M (7/2011)
- Mobile TPV estimated at \$3B in 2011 vs. \$750M in 2010



## PayPal Mobile Services

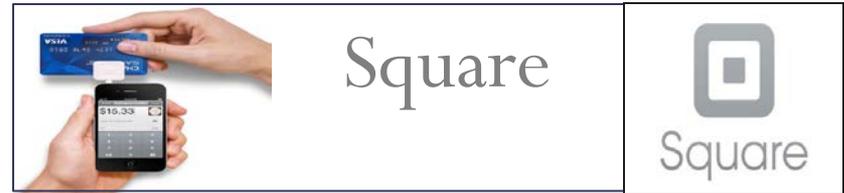
- View PayPal balances and transactions with SMS, WAP or iPhone App
- Mobile P2P to banks, Discover, PayPal account
- POS purchase using phone number/PIN at terminal
  - Access PayPal account stored in Cloud
  - Trial with Home Depot and 15 other retailers
- *PayPal Here* plug-in card reader 



# Other Mobile Payments Disruptors



- **iTunes**
  - 225+ million accounts
  - Mobile payments app
  - Credit card/billing info stored in e-wallet
  - One of the biggest online credit card subscribers
- 100M+ iPhones
- 500,000+ iPhone apps
- Rumors of NFC iPhone
  - Heavy NFC patent activity



- Enables small POS merchants to accept credit/sig debit card payments
- Mobile plug-in device and app
- Payment provider is merchant acquirer, assumes liability
  - Security risk if transactions not encrypted
  - Responsible for charge-backs
- Merchant incentive – lower fees, cash/check replacement
- Competitors include Intuit GoPay, ROAM Data, PayPal Here

# Direct Carrier Billing

- Intermediaries sit between internet merchant and mobile carrier to handle payment to merchant and billing to mobile carrier
- Payment charged to consumer's mobile phone bill as part of monthly billing cycle
- More common in other countries (South Korea)
- U.S. – small value, low risk digital content, online donations
- Issues
  - Bypasses traditional payment process and settlement
  - Risk if purchase value increases or shifts to physical POS
  - Mobile carrier is extending credit, a bank function
    - Make sure vendor billing app is secure and authorized to do billing requests for user
    - Set dollar limits on what can be charged to protect against unauthorized use
    - User parameters to control how, when and by whom they are charged
    - Fraud management and monitoring

**ZONG**

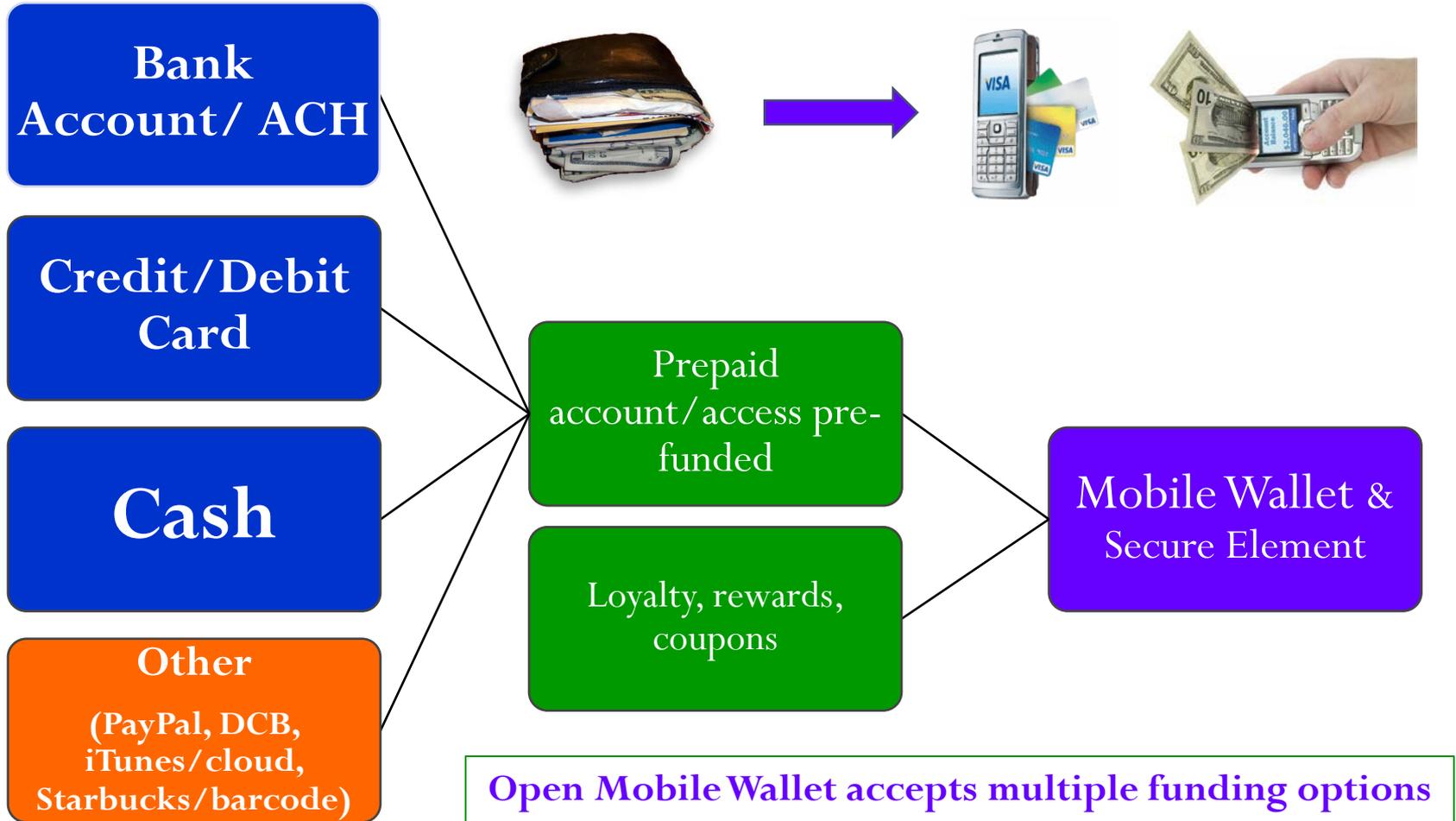
 **BilltoMobile**  
Powered by Datal

 **PayOne**  
Mobile Payments. Mobile Life.

 **PAYFONE**

 **boku**  
Pay by Mobile™

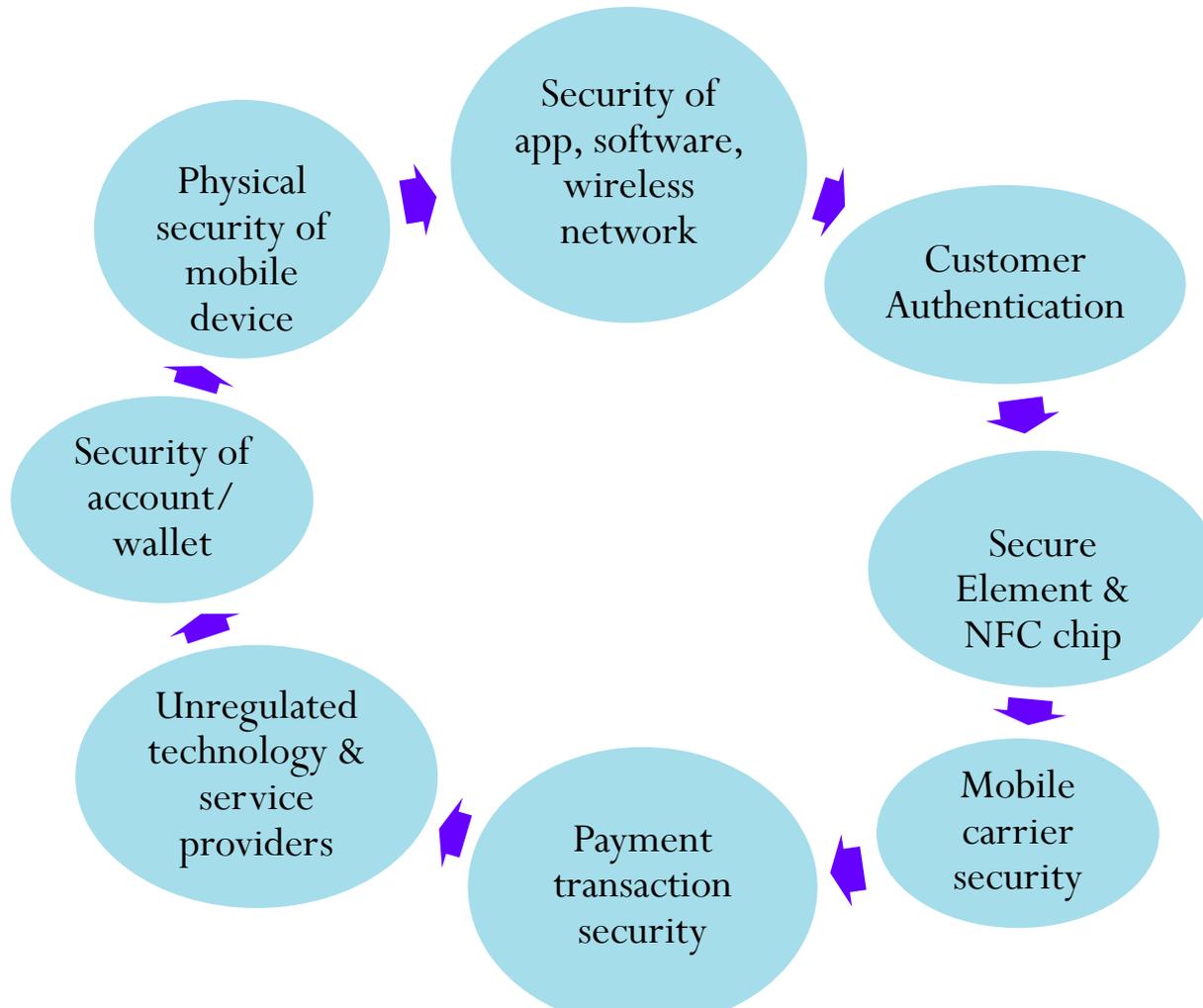
# Future Mobile Wallet



# Mobile Payment Security

---

# Key Mobile Security Checkpoints



- Several potential risk points
- Responsibility for monitoring and protecting must be shared
- Can't be addressed by just one party
- Need to address holistically

# Mobile Payment Security

## Threat

- Poor mobile device security
- Mobile device lost or stolen

# Risks and Mitigation Tools

## Mitigation

- Strong password to access phone
- Multi-factor authentication to wallet
- Remote device deactivation
- Remote wipe and lock
- Auto device log-out
- Auto time-out

- Webroot survey (UK/US 2011)
- Of 1200 mobile users, 40% have security apps; 53% do NOT lock phones

Geo-location finds phone but consumers need to subscribe to these remote services

# Mobile Payment Security

## Threat

- Inadequate fraud controls
- Unauthorized access to device or financial data

# Risks and Mitigation Tools

## Mitigation

- Limit and monitor transaction dollars
- Use alerts to notify customer of suspicious activity
- Encrypt sensitive data stored on mobile device/wallet
- Encrypt transmissions during process and at rest
- Provide consumer education for mobile device and app security
- Develop mobile policies and procedures

# Mobile Payment Security



- Download virus, infected app or malware

# Risks and Mitigation Tools



- Provide ID theft protection (anti-virus software)
- Test and certify applications and mobile vendors
- Create customer guidelines to avoid download of malicious, unsecure or phony apps
- Conduct ongoing mobile risk and control assessments

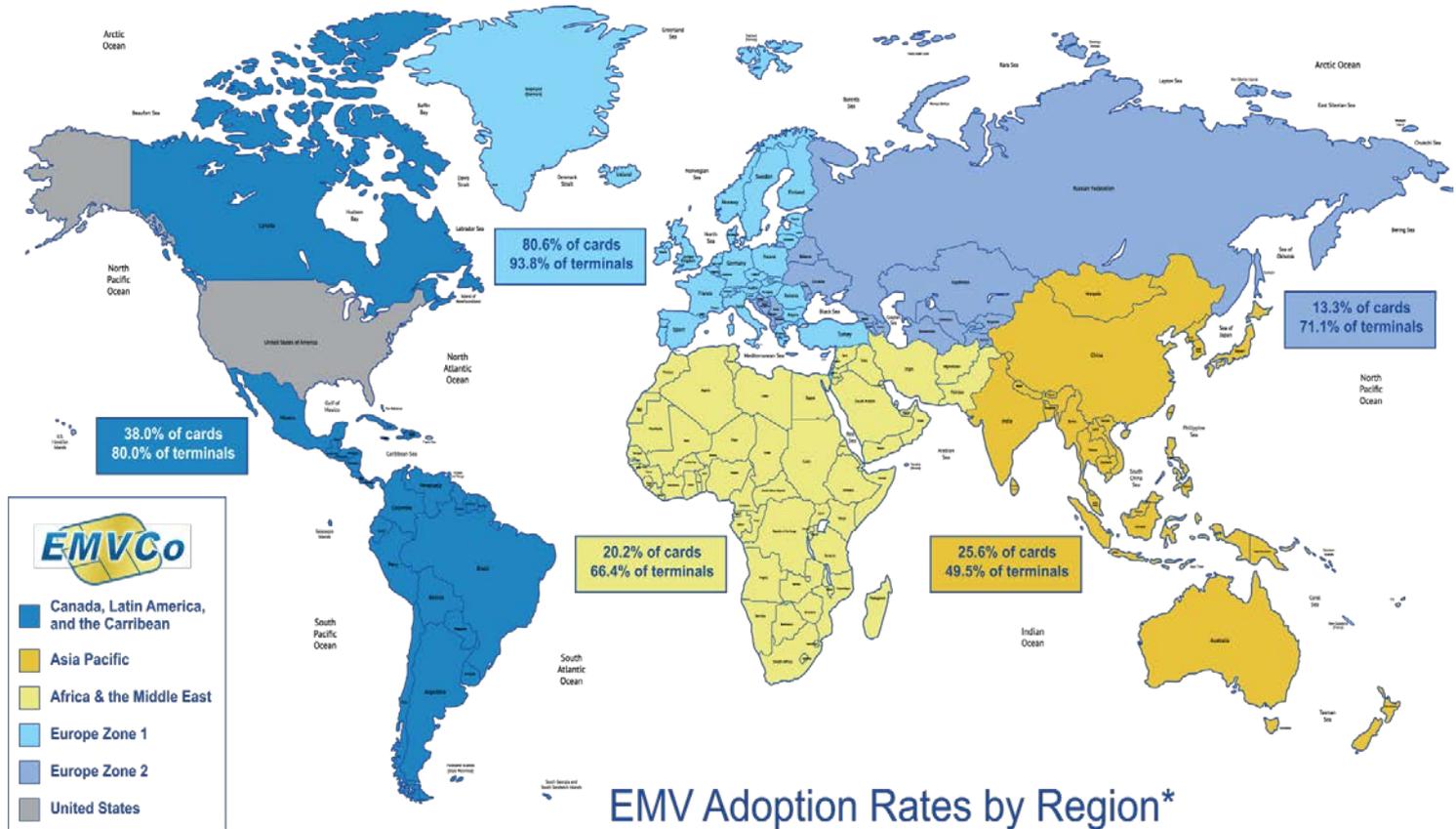
- Need to get consumers to install antivirus & anti malware s/w
- App providers & banks protect software systems from malware by certifying vendors and financial apps loaded to m-wallets

- Overall, need to change customer behavior and get them to share in Risk management

# EMV CHIP + PIN DEBATE

North America  
except U.S.  
Card = 38.0%  
Term = 80%

W. Europe  
Card = 80.6%  
Term = 93.8%



\*Figures reported as of Q3 2011 and represent the latest statistics from American Express, JCB, MasterCard, and Visa, as reported by their member financial institutions globally. Figures do not include data from the United States.

- EMV global standard to replace mag stripe with chip (and PIN) on cards and mobile
  - Chip+PIN vs. Chip only on mobile phone increases fraud protection
- Visa and MasterCard EMV Migration Plan
  - April 2013 acquirers must have EMV-enabled terminals ready
  - Liability Shift effective 10/1/2015

# Why Mobile Payments Can Be Safer

- Users notice their mobile phone is missing 4-8 times sooner than their wallet
- Users almost never leave home without a mobile phone, yet 25-30% leave home without a wallet
- Alerts and responses can be communicated anytime, any place
- Mobile phones have built-in protections
  - Phone has unique numbers associated with phone number (MSISDN), SIM card/subscriber (IMSI) and physical phone (IMEI)
- Consumer has tool to protect phone
  - Consumer selected passcode/PIN
  - Remote deactivation/wipe
- Security credentials on mobile can be tokenized with encryption and dynamic data authentication (DDA)

# Mobile Regulatory Landscape

---

# Regulatory Challenges

- Regulation has not kept pace with mobile payment innovations
- Existing regulations and rules cover underlying payment methods since most non-banks rely on traditional retail funding sources
- Multiple regulatory agencies touch payments and wireless transactions
  - FRS, FDIC, OCC, NCUA, CFPB, FTC, FCC
- Mobile carriers and alternative payment providers unfamiliar with financial services legal requirements:
  - Consumer protection, BSA/AML, KYC, state money transmitters, risk compliance
- FCC oversees mobile carrier standards and competition
- FTC looks at consumer protection and identity fraud more broadly
- CFBP still in learning mode
- Without regulatory coordination of mobile payments, coverage and liability are unclear

# Current Regulatory Landscape

- MPIW met with bank regulators, FTC, and FCC in April, 2012 to discuss **regulatory clarity**, not specific regulation
- Primary concerns – consumer protection, privacy and data security
- Consumer ‘awareness before engagement’
- Important for non-banks and new companies offering mobile services to understand how to protect consumers, but for now banks still liable
- **General consensus – still too early in mobile payments evolution to regulate**
- Focus on education and communication between industry and agencies
- Industry stakeholders want to be involved, in the loop, when need for mobile regulation arises

# Mobile Payment Industry Initiatives

---

# Many New Players in the Mobile Payments Environment

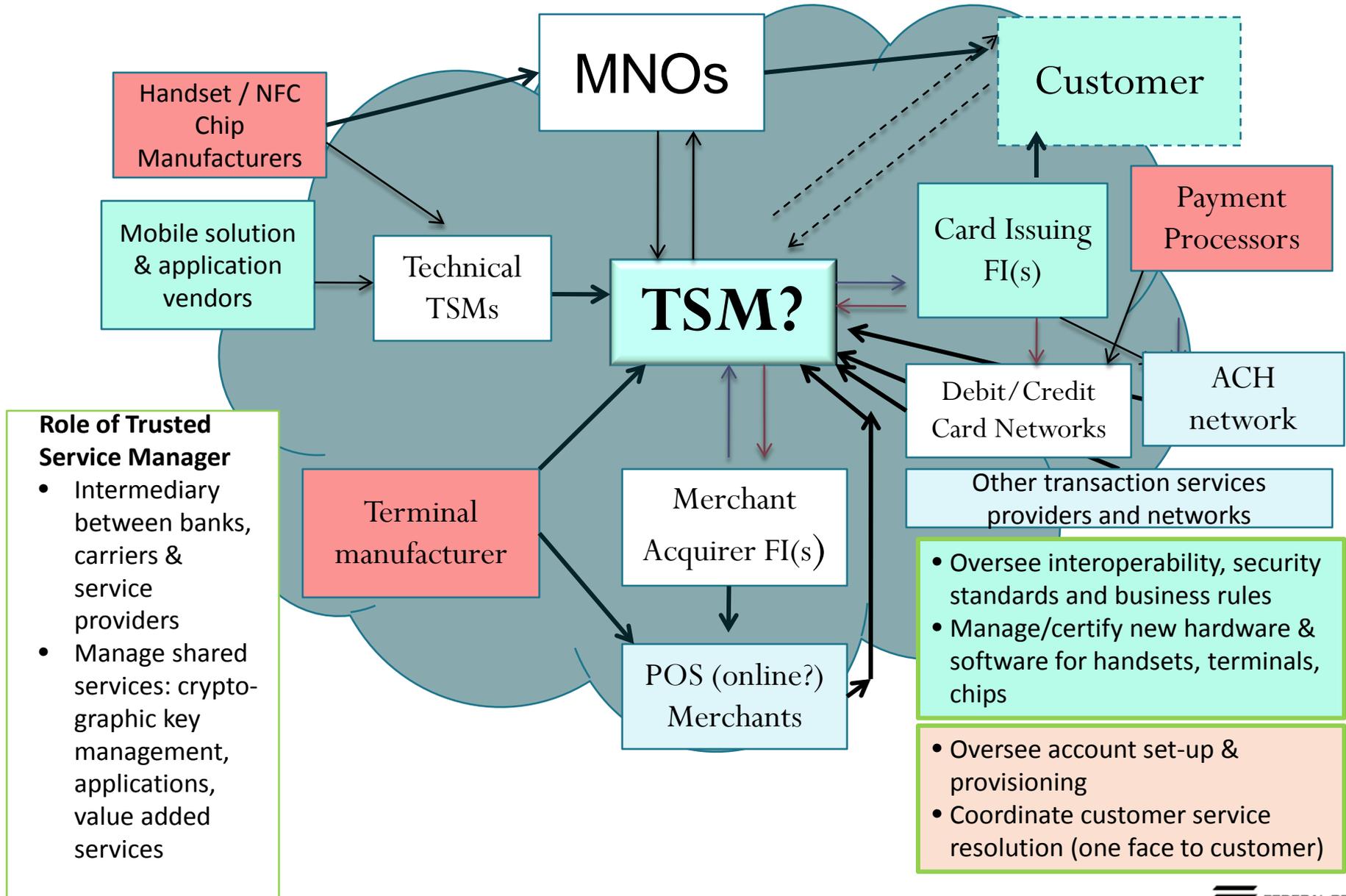
## Traditional Payment System Participants

- Financial institutions
- Customers & merchants
- Payment card networks
- Clearing/settlement organizations
- Third party processors
  - Fiserv, FDC, FIS
- Online payment providers
  - PayPal, Amazon, Google

## New Mobile Technology Participants

- Mobile carriers
  - AT&T, Sprint, T-mobile, Verizon
- Handset/OS manufacturers
  - Apple (iPhone)
  - Nokia, Samsung, Motorola
  - RIM (Blackberry)
  - Google (Android)
- Chip makers
  - Gemalto, DeviceFidelity
- Mobile solution providers
  - Monitise, Clairmail, Intuit, CashEdge, Square
- Carrier billing vendors
  - Boku, Zong, BilltoMobile

# Collaboration is Challenging



# Evolution of Mobile Payments Industry Workgroup (MPIW)

- 2010 – Fed convened mobile payment stakeholders to address fragmentation and encourage communication on direction of mobile payments in U.S.
- Wanted to understand industry perspectives on mobile payment developments in U.S. and expectations of Federal Reserve
- Established MPIW objectives
  - Create dialogue and transparency among participants to better understand industry roles in the evolving U.S. mobile payments ecosystem and build relationships
  - Build consensus on mutual points of value, challenges and opportunities in mobile payments
  - Discuss possible business cases for collaborative activities to help build critical mass for mobile payments
  - Establish a manageable scope of action for the MPIW going forward



# Mobile Payment Opportunities and Challenges

## Opportunities

- More security options
- Merchant efficiencies
- Consumer convenience, demographic & life style changes
- Marketing & location-based services (LBS)
- Convergence with value-added services
- Financial inclusion

## Challenges

- Lack of consumer demand
- Business model revenue sharing
- Customer (and data) ownership
- Merchant business case *weak*
- Collaboration of many stakeholders
- Few NFC phones in U.S.
- Lack of global standards
- Unclear regulatory direction

# Principles of a Successful U.S. Mobile Payments Framework

- Open mobile wallet that supports multiple payment options
- NFC technology for contactless mobile payments at POS
- Existing clearing and settlement channels (credit, debit, ACH, prepaid and carrier billing) to ensure ubiquity, mass adoption and consumer choice
- Dynamic Data Authentication for security/fraud prevention
- Based on global standards and an industry certification process
- Regulatory clarity to avoid gaps in oversight and consumer protections between agencies & addresses standards for security and processes
- TSMs to oversee security and account management functions

# Fed/MPIW Status – 2012

- Fed, MPIW and other mobile industry experts testified at House and Senate hearings in March 2012
- Fed will publish report on *End-to-end Risk Management & Security Requirements for NFC and Cloud Mobile Payments* and update the 2011 *Mobile Payments in the U.S.* whitepaper later this year
  - <http://www.bostonfed.org/bankinfo/firo/publications/bankingpapers/2011/mobile-payments-mapping.htm>
- Fall 2012 MPIW meeting will include session with merchants and possibly mobile start-ups
- MPIW and Fed will continue dialogue with regulators to clarify oversight responsibilities, help create regulatory guidelines for security and privacy; and work on developing business standards and best practices
- Participate in development of industry-wide mobile payment standards

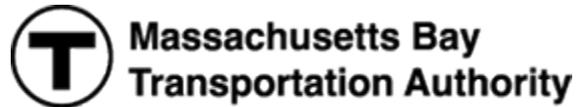
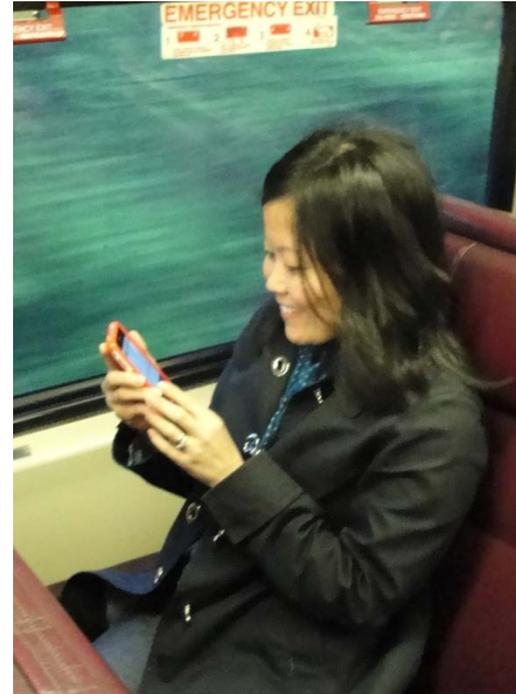
# Conclusions

- Non-banks will continue to play strong roles in innovation and implementation of mobile services and technology
- More partnerships with mobile stakeholders likely as nonbanks and financial institutions jockey for position and wallet share
  - Banks help shape mobile market, mitigate risks, maintain customer relationships
- Security and fraud issues must be addressed collaboratively to reach full adoption of mobile payments
  - Include risk monitoring, fraud prevention, and education of banks, carriers, vendors, merchants and consumers
- Consumers will adopt mobile payments, regardless of provider, if they meet requirements for convenience, security and incremental value
- Banks should work with mobile industry groups to develop technical, business and security standards, and effective consumer education tools
  - Mobile Payments Industry Workgroup, Mobey Forum, NFC Forum, Smart Card Alliance, ANSI X9, NACHA, etc.

# **A Day in the Life ... Mobile Payments @ Work**

---

# Getting to work ...



**Massachusetts Bay  
Transportation Authority**

Mobile ticketing app  
(coming soon)

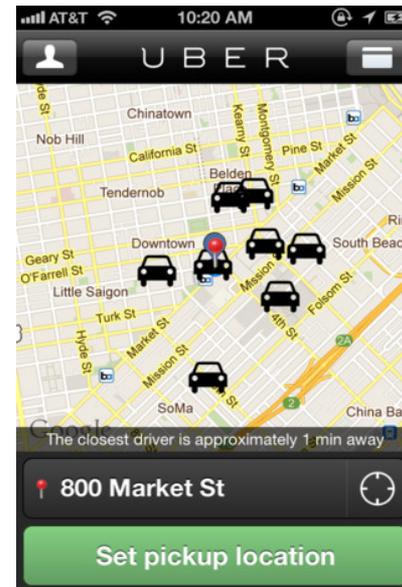
# ... Morning ...



Sage Payment Solutions



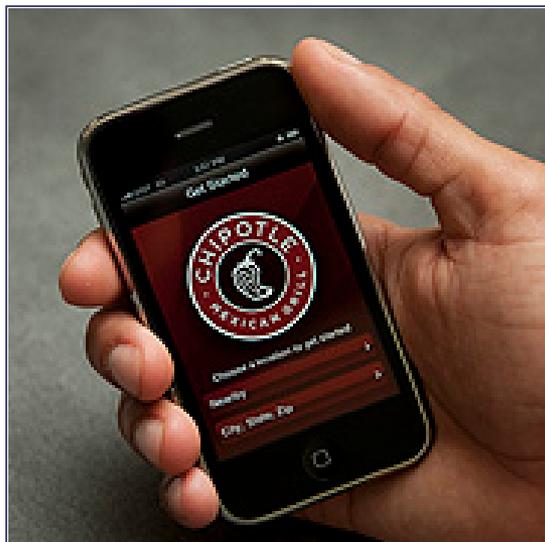
# ... Afternoon ...



# ... Evening



by AisleBuyer



# Tabbedout®