U.S. Mobile Payments

Mark MacCarthy

November 2009

U.S. Market: Contactless

- Visa PayWave
- MasterCard PayPass
- American ExpressPa
- Issuers
- Merchants
  - Convenience, speed
- Limited deployment

U.S. Market: Mobile

- POS terminals compatible with contactless
- Not deployed in US phones
- Decision up to US carriers
- Contactless stickers and SIM card

U.S. Market: Prospects

- Key driver will be merchant POS upgrade
- Existing infrastructure works well for both consumers and merchants
  - Are benefits worth the extra cost?
- Carriers as payment intermediaries
  - Driver would be interchange revenue
  - Limited engagement through digital content
  - Regulatory status?
  - Liability?

Policy

- Security
- Privacy Concerns
- Consumer Protections

Contactless Functioning

Card to terminal communication



Security

- Magnetic Stripe Card Payment Processing
  - Role of CVV
- Contactless and Mobile Processing
  - Role of dynamic CVV
- Key point: value of security code changes with each transaction
- Even if information is intercepted it cannot be used to make another card or transaction

Privacy

- No new privacy risk currently
- Same information is transmitted in both magnetic stripe and contactless transactions
- Possible privacy risk if payment information is combined with location information

RFID Privacy Regulation

- Payment applications included
- EU Recommendation
- Not clear it should apply to payment card application
  - Requirement to disable RFID chips at POS
  - Notice

Consumer Protection

- Mobile payment application processed by traditional payment card networks
  - Existing consumer protections apply
    - Limited liability, redress and dispute rights
- Other payment intermediaries
  - Protections voluntary
  - CTIA Mobile Financial Services code:
    - MFS Providers of mobile payment systems should create policies that cap liability for unauthorized transactions. Such policies should, at a minimum, comply with liability caps required under existing legal requirements