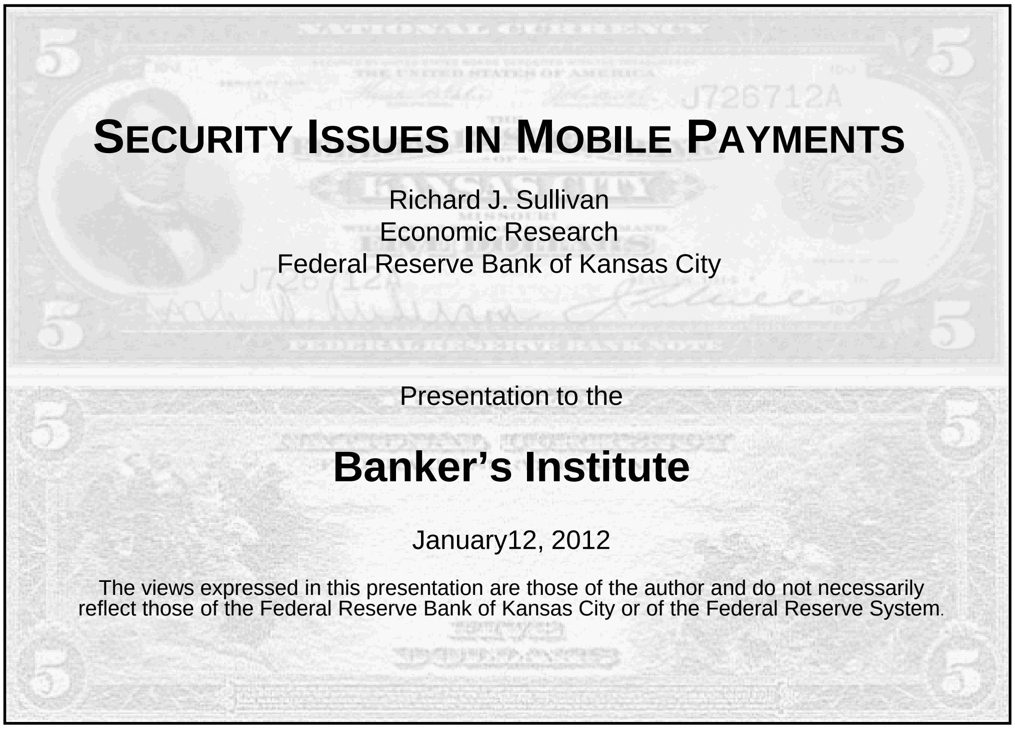


Security Issues in Mobile Payments

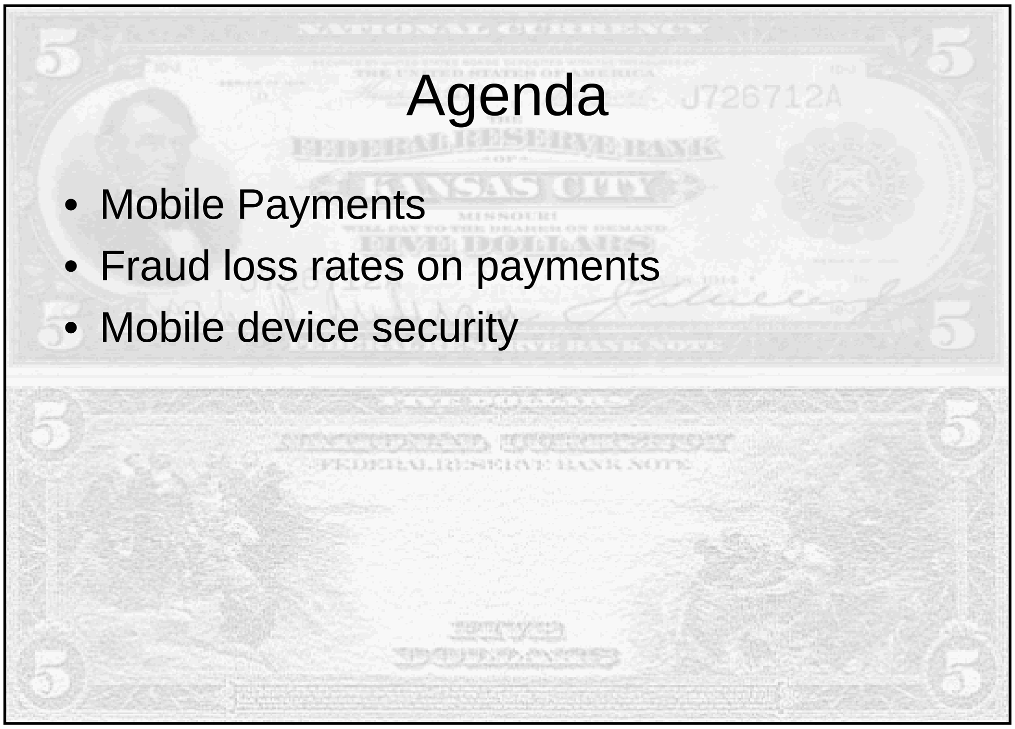
Richard J. Sullivan
Economic Research
Federal Reserve Bank of Kansas City

Presentation to the

Banker's Institute

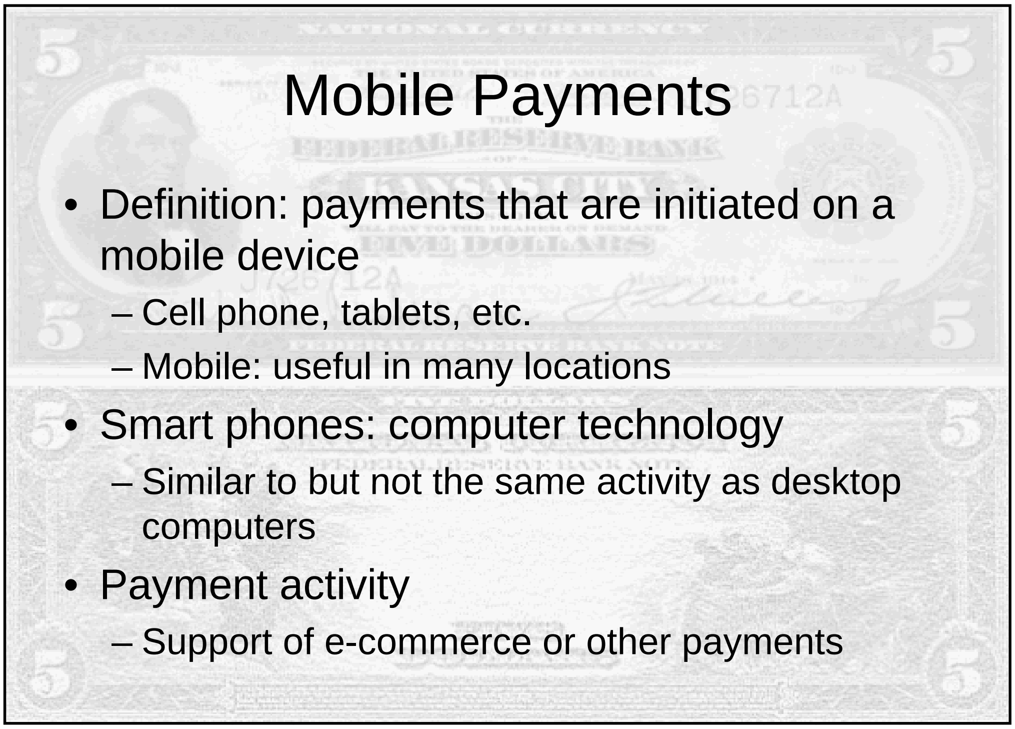
January12, 2012

The views expressed in this presentation are those of the author and do not necessarily reflect those of the Federal Reserve Bank of Kansas City or of the Federal Reserve System.



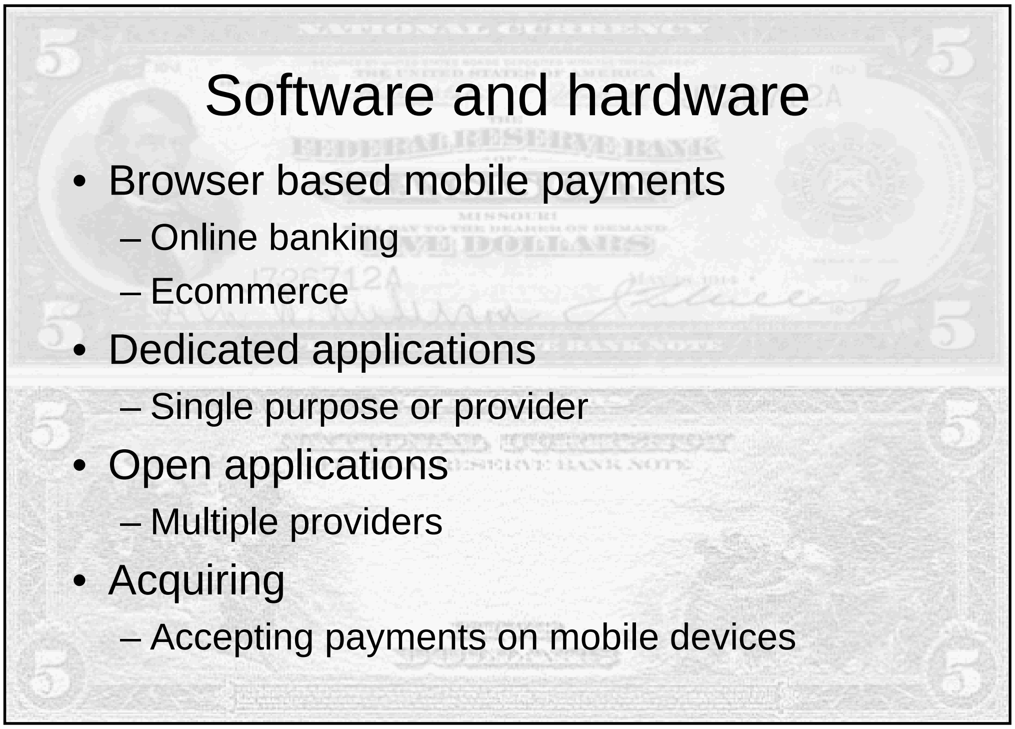
Agenda

- Mobile Payments
- Fraud loss rates on payments
- Mobile device security



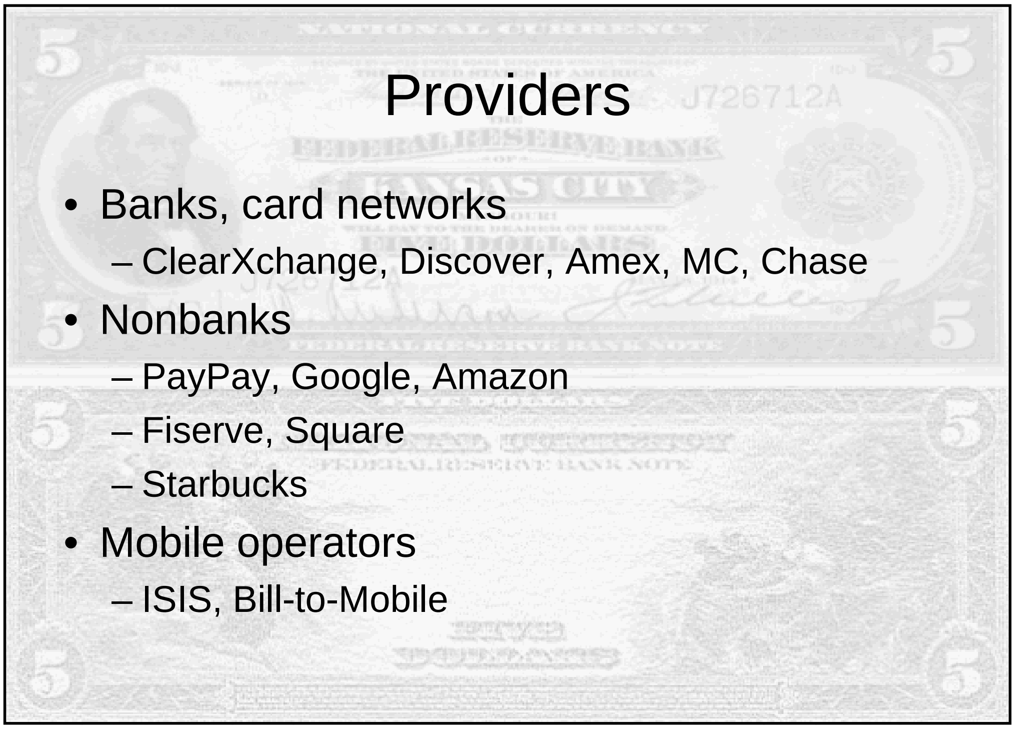
Mobile Payments

- Definition: payments that are initiated on a mobile device
  - Cell phone, tablets, etc.
  - Mobile: useful in many locations
- Smart phones: computer technology
  - Similar to but not the same activity as desktop computers
- Payment activity
  - Support of e-commerce or other payments



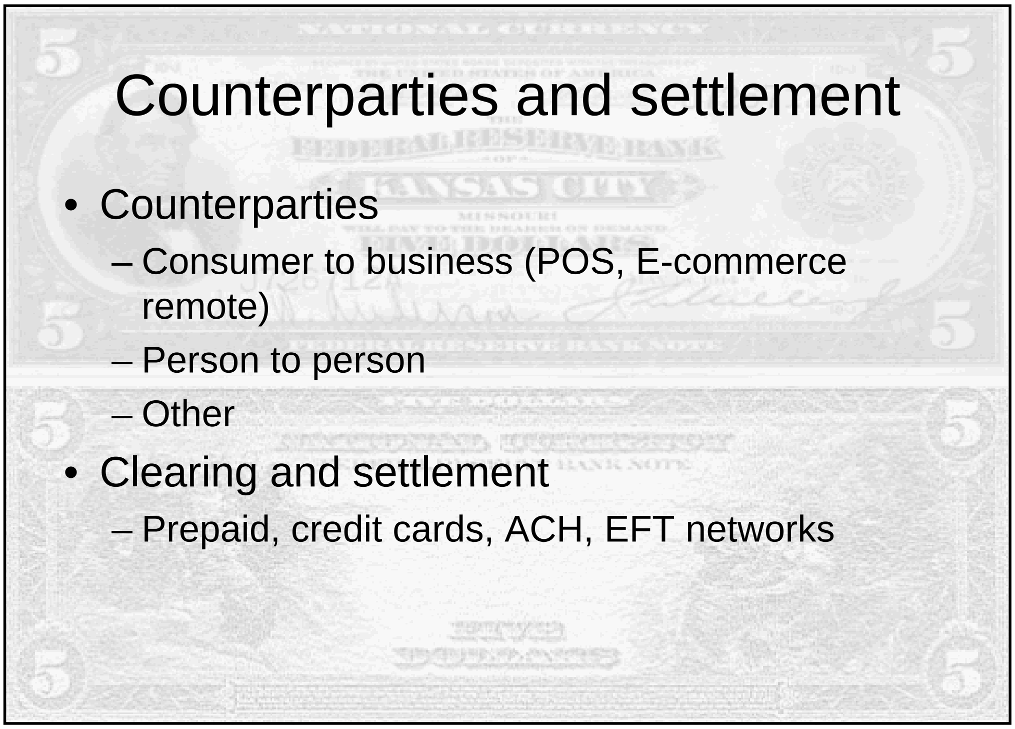
Software and hardware

- Browser based mobile payments
  - Online banking
  - Ecommerce
- Dedicated applications
  - Single purpose or provider
- Open applications
  - Multiple providers
- Acquiring
  - Accepting payments on mobile devices



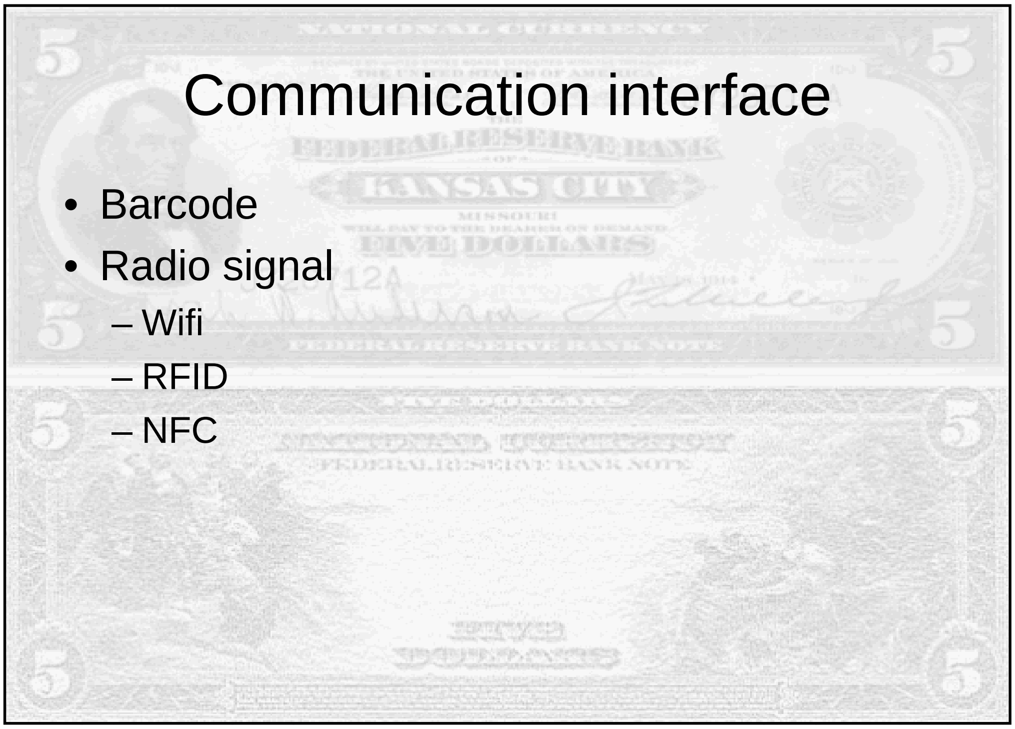
Providers

- Banks, card networks
  - – ClearXchange, Discover, Amex, MC, Chase
- Nonbanks
  - – PayPay, Google, Amazon
  - – Fiserve, Square
  - – Starbucks
- Mobile operators
  - – ISIS, Bill-to-Mobile



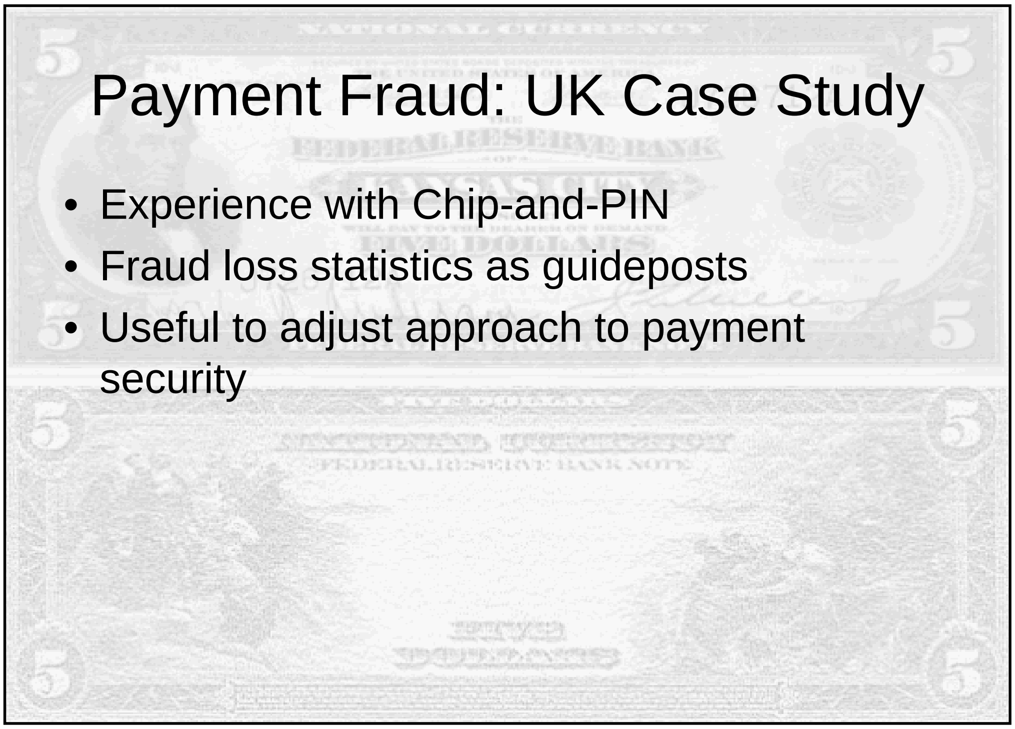
Counterparties and settlement

- Counterparties
  - – Consumer to business (POS, E-commerce remote)
  - – Person to person
  - – Other
- Clearing and settlement
  - – Prepaid, credit cards, ACH, EFT networks



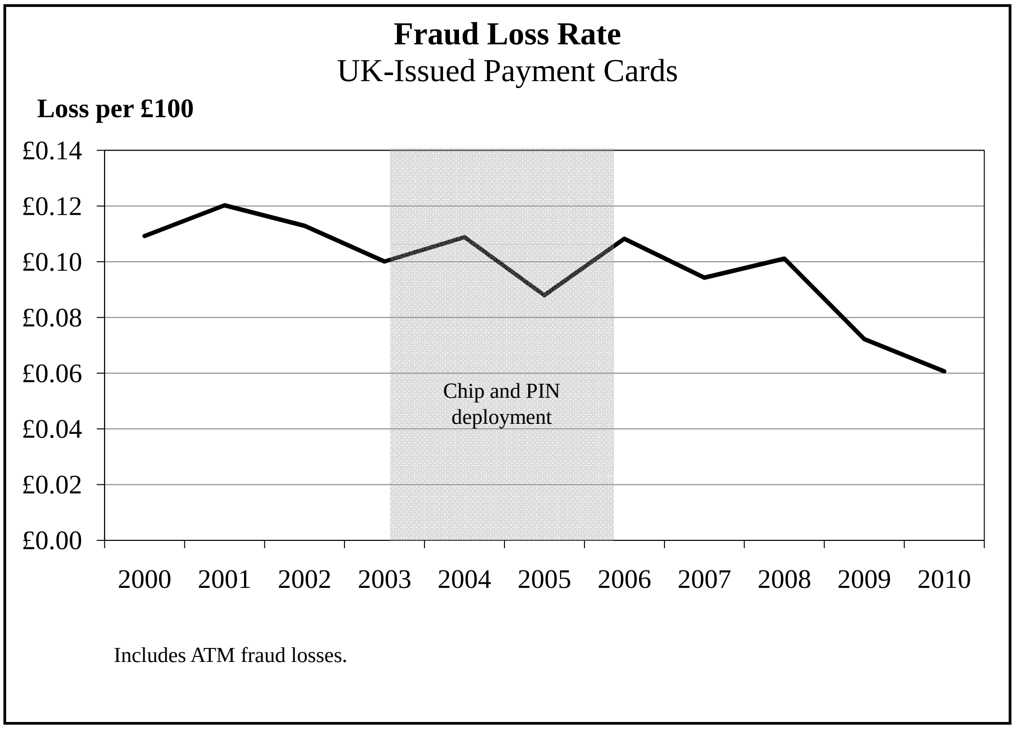
Communication interface

- Barcode
- Radio signal
  - – Wifi
  - – RFID
  - – NFC



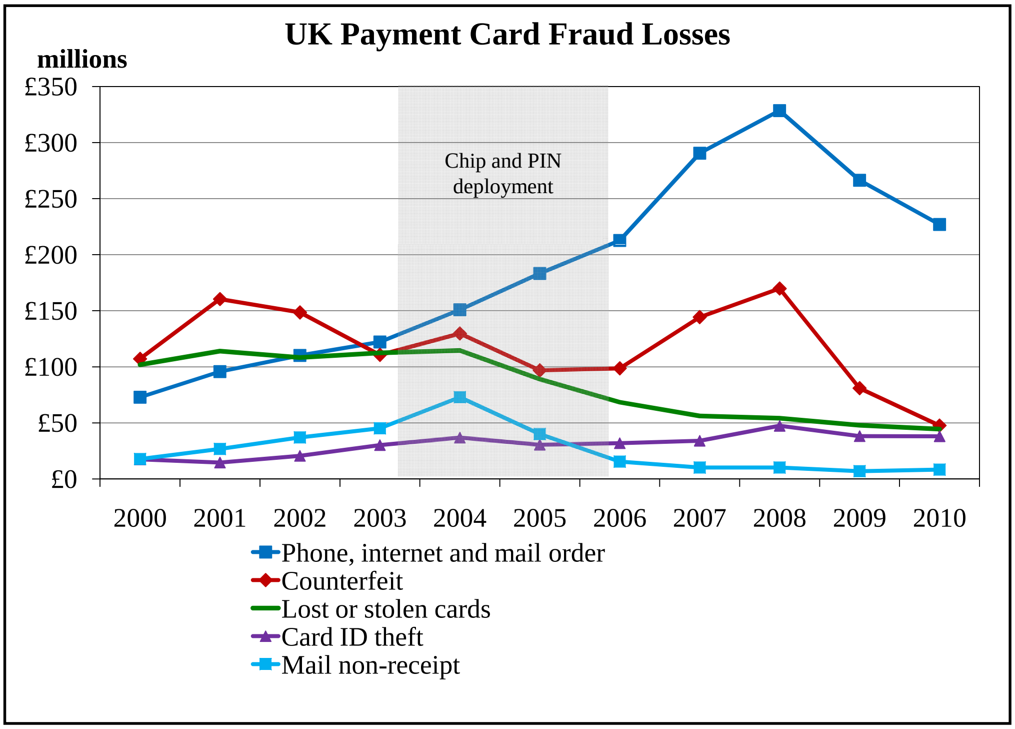
Payment Fraud: UK Case Study

- Experience with Chip-and-PIN
- Fraud loss statistics as guideposts
- Useful to adjust approach to payment security

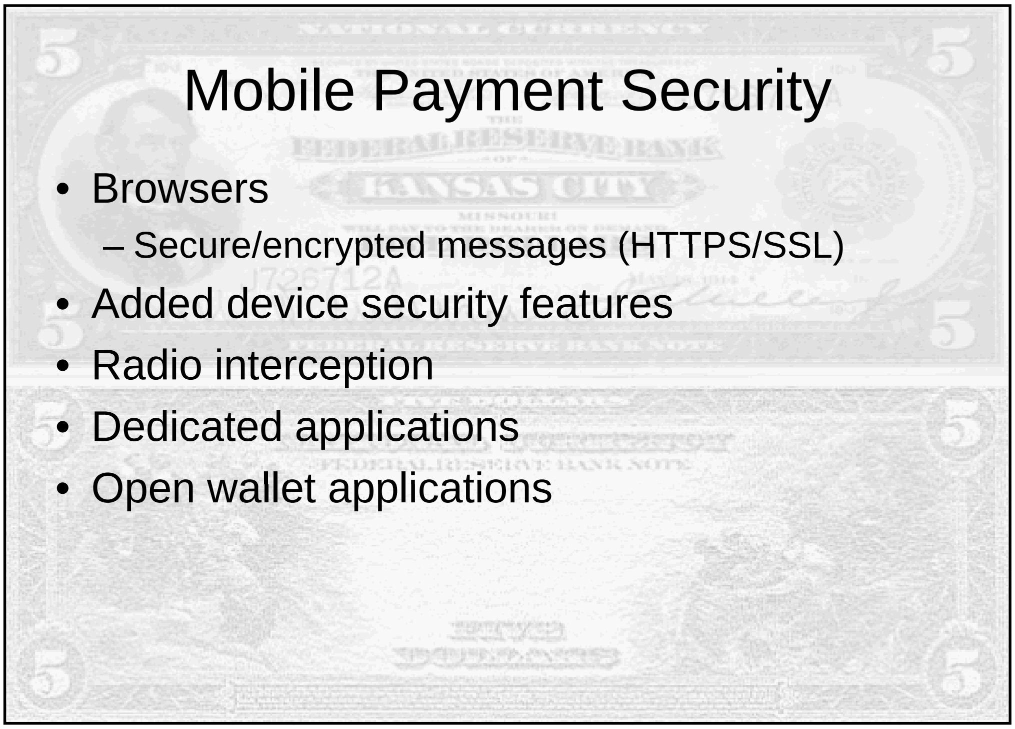


Fraud Loss Rate
UK-Issued Payment Cards

Includes ATM fraud losses.

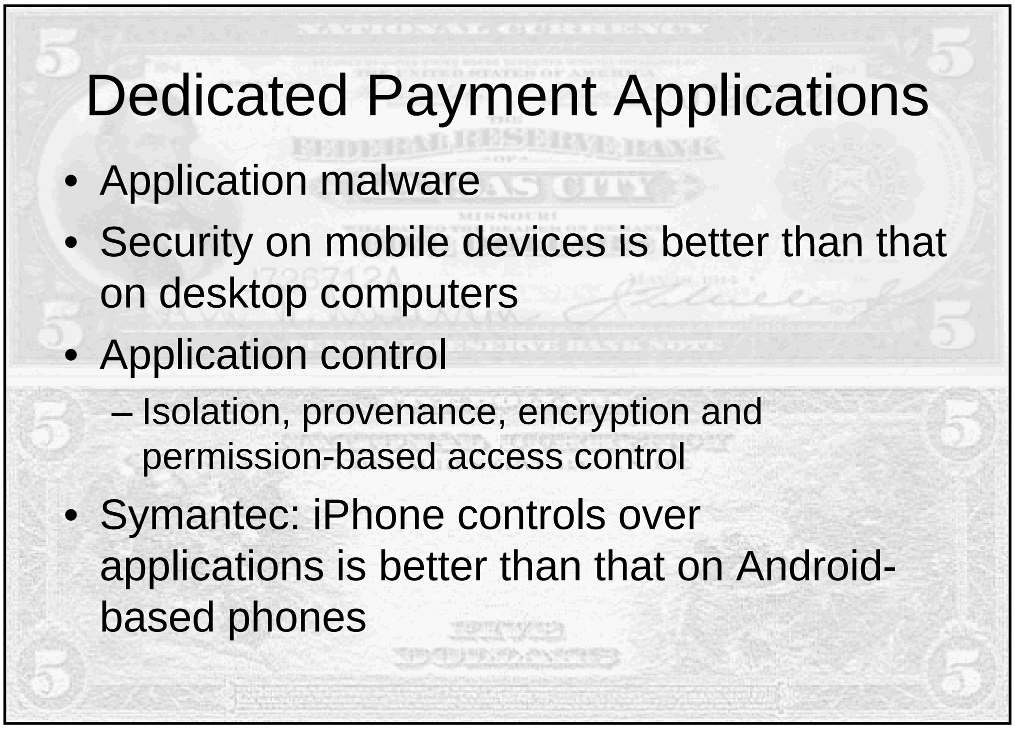


UK Payment Card Fraud Losses



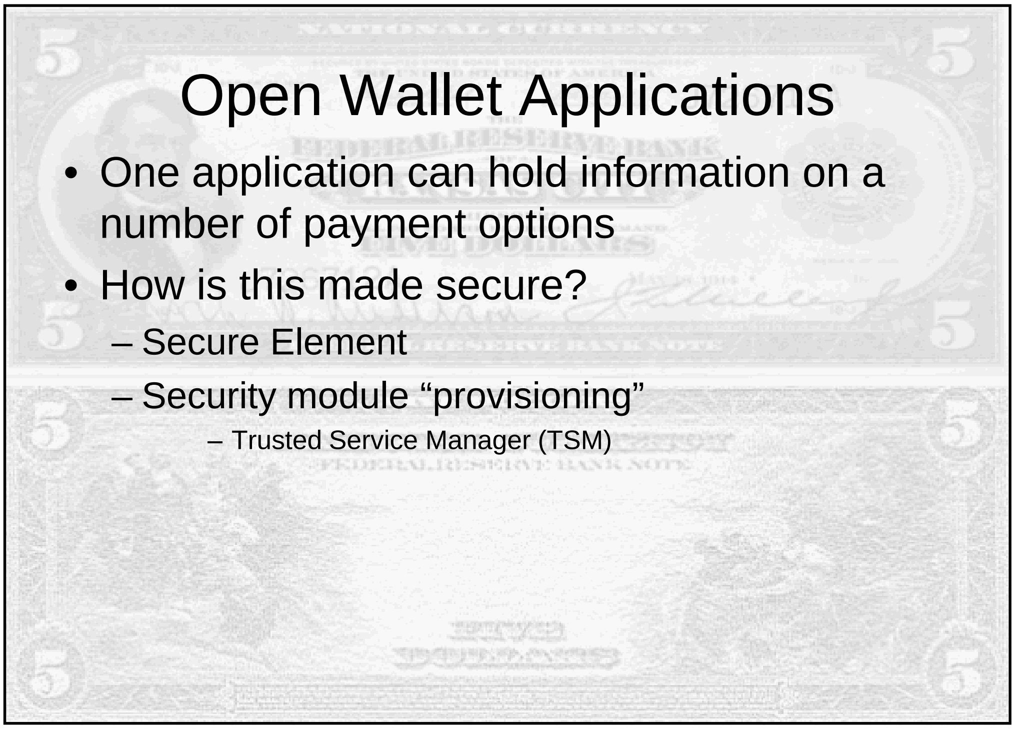
Mobile Payment Security

- Browsers
  - Secure/encrypted messages (HTTPS/SSL)
- Added device security features
- Radio interception
- Dedicated applications
- Open wallet applications



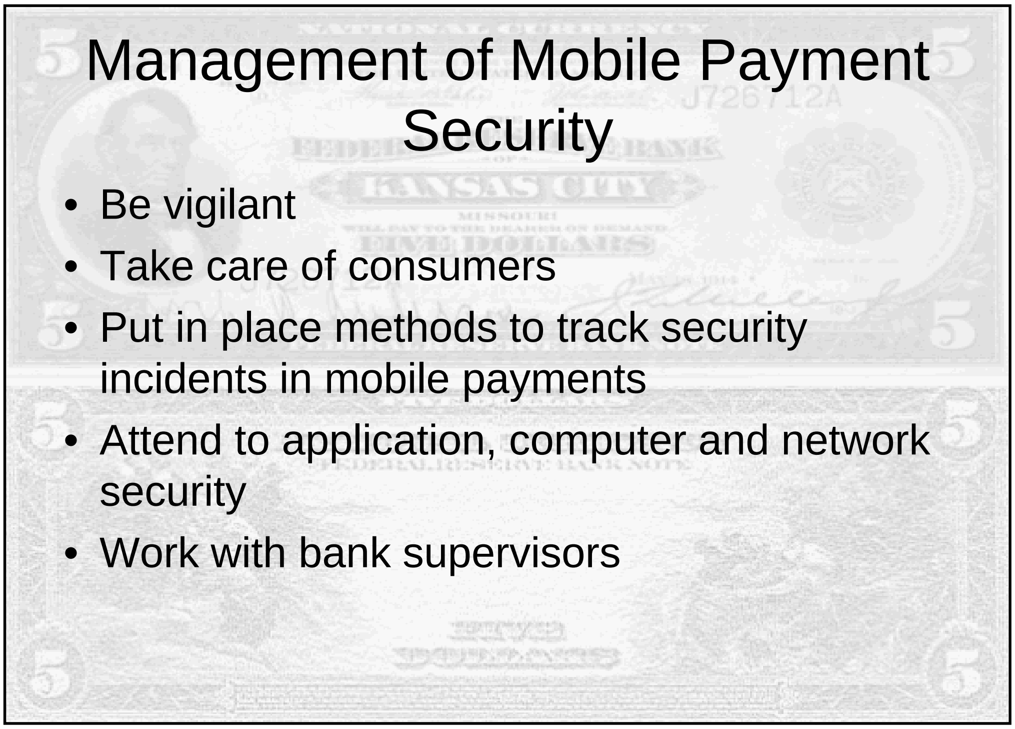
Dedicated Payment Applications

- Application malware
- Security on mobile devices is better than that on desktop computers
- Application control
  - Isolation, provenance, encryption and permission-based access control
- Symantec: iPhone controls over applications is better than that on Android-based phones



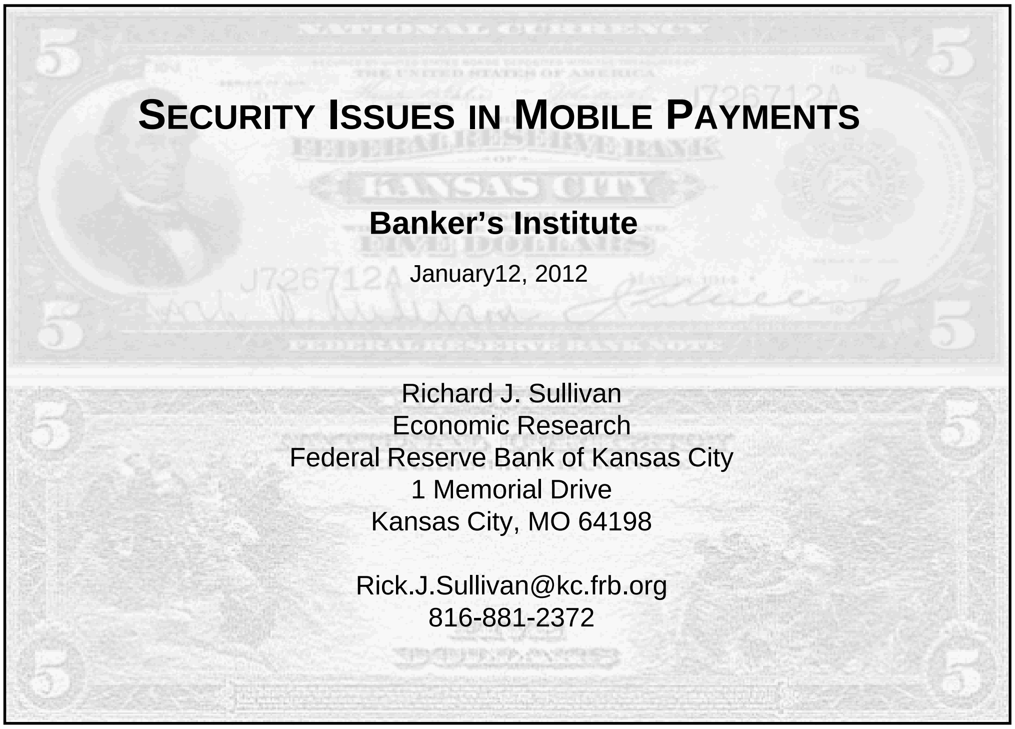
Open Wallet Applications

- One application can hold information on a number of payment options
- How is this made secure?
  - – Secure Element
  - – Security module “provisioning”
    - – Trusted Service Manager (TSM)



Management of Mobile Payment Security

- Be vigilant
- Take care of consumers
- Put in place methods to track security incidents in mobile payments
- Attend to application, computer and network security
- Work with bank supervisors



SECURITY ISSUES IN MOBILE PAYMENTS

Banker's Institute

January12, 2012

Richard J. Sullivan
Economic Research
Federal Reserve Bank of Kansas City
1 Memorial Drive
Kansas City, MO 64198

Rick.J.Sullivan@kc.frb.org
816-881-2372