Very glad to be here.

Four observations
1. Dynamics of card payment approval
2. The promise of PCI has not been realized
3. Options for the future: digital two-factor authentication
4. Potential government oversight

Note disclaimer. Me: Fed 17 years. 9 with banking supervision, the rest in payments research; bank risk a common theme to my research

1. Dynamics of card payment approval
   -Fraudsters are gaming ecommerce merchant screening systems, sending “clean” transactions to merchants (Cybersource)
   -Accurate billing address and card verification codes, botnets submitting orders to disguise location, reshipping services to provide a variety of delivery addresses
   -Recommendation: get more data, do more sophisticated analysis for screening

Problem: information-intensive card payment approval leads to an escalating cycle of information defenses and information attacks

Diminishing returns?
2. Current strategy: protect data

• The promise of PCI has not been realized
  • Breaches at retail and commerce companies (DLDB)
  • Peak year for incidents—2008 at 190 breaches (CHART)
  • In 2010, only 73 breaches—decline of 38%
  • Reversal of trend: Through June 2011, 70 incidents that has exposed 105
    million records

• PCI compliance are near 100% for level 1 merchants, and there has been progress
  in smaller merchants

  • PCI is stumbling
  • Higher levels of compliance does not appear to be holding back the hackers
  • Must expect a wave of fraud from this stolen information, much of which will
    target ecommerce and CNP transactions
3. UK experience: increase in counterfeit and CNP fraud after EMV adoption
   • But what caused CNP fraud to decline? Maybe 3D secure?
     • 2008: “uptake of Verified by Visa is low” (The Register); customers unhappy about being forced to use 3D secure;
     • 2011: BRC—50% of UK issued cards are “enrolled and regularly use 3D secure”; some acquirers make 3D secure a condition for a merchants contract; merchants are “incentivized” to use 3D secure
   • Digital two-factor authentication
     • Something known, something secret
     • 3D Secure, PIN debit online, Secure Vault Payments (SVP), PayPal
     • Does not rely solely on public information
4. Government oversight
   • Existing authority
     • Bank regulation/supervision: supervisors nudged banks to upgrade internet banking security
       • Model: require upgrades but be agnostic on the exact technology
       • Could something similar be done with payment security?
   • Is new authority needed?
     • Maybe: bank supervision does not directly affect retailers
     • Most important: coordination/chicken-and-egg problem—all merchants need to upgrade security to avoid competitive disadvantage.