Defending Debit

Indirect Effects of the Durbin Amendment on Investment in Debit Card Security

Allison Miller
The Society of Information Risk Analysts
Prepared for WEIS 2014 (June 23, 2014)

Overview

- Interested in understanding how payment network participants make investment decisions around risk mitigation (security/fraud)
- Examined the Durbin amendment, which affects large debit card issuers in the U.S., to see if the externality affected risk management/security investment
- Used the 2013 Q4 breach events as a case study to discern changes in response behavior, investment strategy

Card Issuance (Debit) Model

- Debit cards provide customers with an access mechanism to funds in their bank account
  - PIN or signature-based "authentication"
  - ATM or Branded (e.g. Visa, MasterCard) network processing
- Debit business model
  - Banks earn revenue when customers use their cards at the point-of-sale; merchants pay transaction fees (e.g. interchange)
    - While credit card issuers earn revenue off of interest on credit lines, debit issuers rely more on transaction and account fees
  - Transaction fees often subsidize bank account services (e.g. free checking)
  - Branded (signature) network processing more expensive/lucrative than ATM/regional (PIN-based) network processing
    - In 2013 the avg credit card interchange for a Visa premium, card present txn was about 2.1%
    - A similar PIN-based txn earned issuers about $0.30 per txn, approximately 0.69%

The Durbin Amendment

- Part of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010
- Specific to debit card processing
- High-level overview
  - Dictates price banks charge merchants (interchange) for signature debit products
  - Disallows bank (issuer) control over debit card transaction routing
- Exemptions
  - Banks w/assets < $10B USD (e.g. credit unions)
  - "Prepaid" debit products

Issuer Breach Response

- **Reactive options**: Reduce fraud associated w/a single breach, typically short-term steps, short-tail of effectiveness
  - Reissuance - replace cards
  - Caps & Compromised Card Strategies - simple restrictions
  - Restricting Authorization Strategies - sophisticated restrictions
- **Proactive options:** reduce fraud risk exposure (in general), long-term horizon, long tail
  - Advanced Authorization Systems - faster/smarter/better data
  - Acceptance-Side Prevention - for issuers, typically card (or the more abstract "payment method" based risk controls: CVV, CSC, AVS, Chip & PIN, Chip & Sig, 3D Secure

Durbin's Affect on Risk Exposure

- Fraud loss exposure of issuers now different (higher):
  - When a transaction occurs, the issuer earns interchange (for example, 2%)
  - With fraud, issuers lose the face value minus the processing fees received (98%)
  - For every fraudulent $100 transaction, 49 equivalent $100 transactions needed to "break-even"
  - If fees are halved, double the number (i.e. 98) of transactions needed to "break even"
- For Debit: upside is closer to flat, downside is relative:
  - A debit card issuer has a higher risk exposure, in both absolute terms and relative to the potential revenue
    - On a $2000.00 transaction there's a $1.22 upside, $1998.78 downside (exposure = 1638x upside)
    - On a $2.00 transaction there's a $0.22 upside, $1.78 downside (exposure = 8x upside)
  - To keep (absolute) costs of fraud losses stable, current fraud prevention practices suffice
  - To keep impact of fraud stable, issuers are likely to be more sensitive to high-dollar transactions, or use strict limits to curtail exposure above a certain threshold

BREACH RESPONSE: POST DURBIN

- **Holiday season 2013 breaches:**
  - ~40M cards breached at Target alone, with >$170M costs in breach response and >17.2M cards reissued as of February 2014

	Credit	Debit
Reactive options		
• Reissuance - replace cards	X	X
• Caps & Compromised Card Strategies		X+
• Restricting Authorization Strategies	?	?
Proactive options		
• Advanced Authorization Systems	Ongoing	Ongoing
• Acceptance-Side Prevention	X	

FINDINGS

Pre-Durbin: In the U.S., credit and debit issuers had similar security, fraud prevention, and breach response practices

- However regarding EMV chip implementation, credit issuers appear to be more likely to have adopted chip than debit issuers

Durbin: The Durbin Amendment does not specify requirements to Issuers related to security, fraud prevention, or breach response

- However fees earned on debit interchange are both (on average) lower and also more flat, with a penny of the average $0.22-0.25 in fees allocated to fraud prevention for qualifying issuers.

Post-Durbin: We observed differences in debit issuer breach response, as debit issuers appeared more likely to impose spending limits/caps, and a large debit provider engaged in a new process as part of the breach response: publicizing their changed authorization strategy

- Also, some issuers have announced expedited plans to upgrade acceptance infrastructure to EMV chip, but in reference to their credit – not debit - cards

FINDINGS

- Post-Durbin, Debit Issuers appear to be:
  - Loss resistant: More sensitive to loss exposure in the short-term, and may be more willing to forego potential revenue to maintain transactional risk exposure at acceptable levels (compared to credit issuers)
  - Cost avoidant: Less interested in long-term investment to reduce overall risk exposure
- Other observations related to security/investment in infrastructure in the payments industry:
  - Large breaches seem more frequent, but system-wide fraud rates at near-lows
  - Transactional fraud liability, the typical approach used to solve participant coordination issues, may not be as useful for systemic/distributed exposure issues (e.g. 3D Secure)
  - Viable alternatives to compliance programs require additional research, may require new types of incentives to gain traction

CONCLUSION

- The Durbin amendment's affect on debit card issuers' margins appear to have affected both their risk/loss tolerance and propensity to invest in fraud/security infrastructure
- It is unclear if the transactional fraud liability shift alone will provide enough incentive to drive investment in stronger acceptance infrastructure, and debit card issuers specifically may need additional incentives
- If a policy goal is to improve payment system security, recent breach activity suggests additional incentives beyond transactional fraud liability and compliance schema are needed, especially in the face of negative externalities