CONSUMER REACTIONS TO DATA BREACHES

Claire Greene
Eric Johnson
Slava Mikhed

NACHA Payments 2017
April 24, 2017

DID THE TARGET BREACH CHANGE CONSUMER ASSESSMENTS OF PAYMENT CARD SECURITY?

Claire Greene
Presented to NACHA Payments 2017
April 24, 2017

CPRC CONSUMER PAYMENTS Research Center
FEDERAL RESERVE BANK OF BOSTON™

Disclaimers

- The views expressed in this presentation are those of the author and do not necessarily represent the views of the Federal Reserve Bank of Boston or the Federal Reserve System.

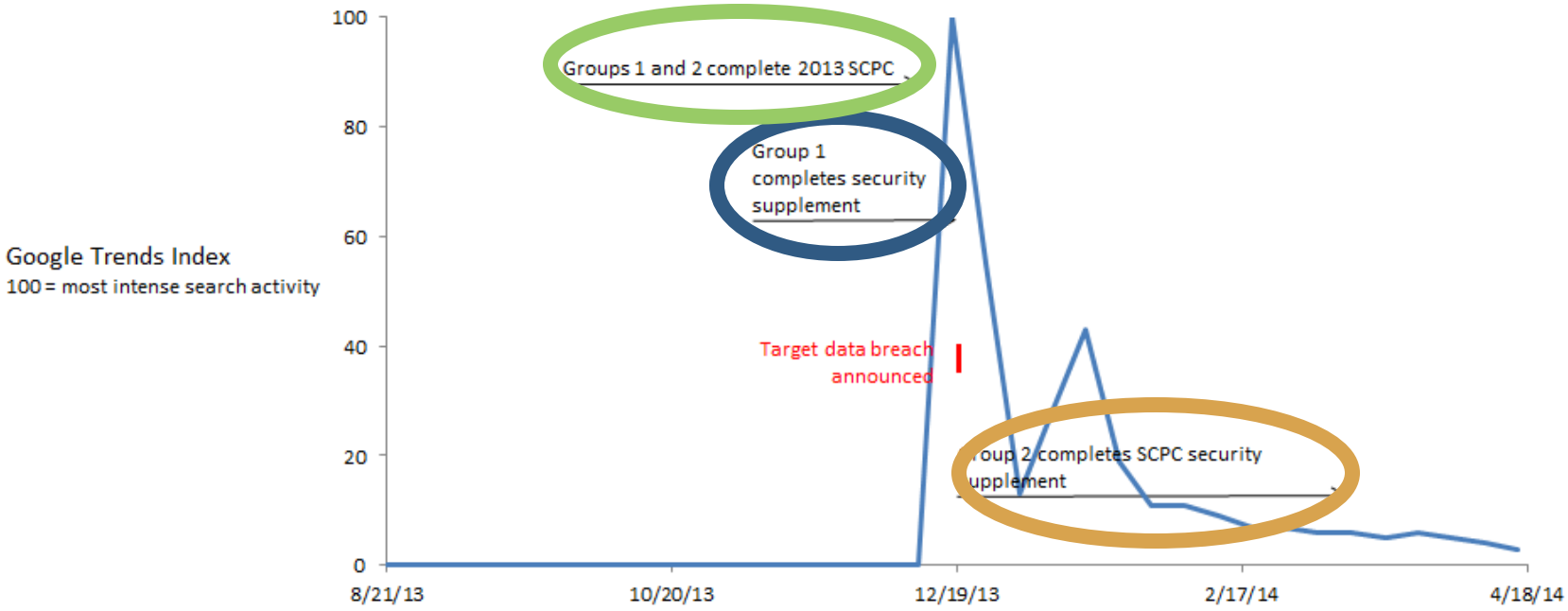
Target data breach

- Payment card data for 40 million credit and debit card accounts
- Used in Target stores in the 19 days between November 27 and December 15, 2013
- Announced December 19, 2013

Research question

- Does news about payment security breaches change the way consumers assess and use payment instruments?

Timeline of data collection



Source: Federal Reserve Bank of Boston, Google Trends.

Note: 100 equals most intense search activity on “Target data breach.” The spike in searches occurred almost instantaneously following announcement of the breach; software limitations cause it to appear on the figure to have begun slightly in advance of the announcement.

Survey of Consumer Payment Choice

- Annually since 2008
- Online survey
- Conducted in the fall
- 2,000+ U.S. consumers
- Adults age 18+
- Best practices of panel recruitment
- Many respondents take survey in multiple years
- Detailed demographic info: income, age, education, race, etc.
- Measures adoption and use of payment instruments
- Respondents also rate payment instruments on characteristics

Survey asks: In a “typical” month…

How many?

Bill payments

1. Automatic
2. Online
3. In person, by mail or phone

Nonbill payments

4. Online
5. Retail goods
6. Retail services
7. P2P

Paid by each instrument?

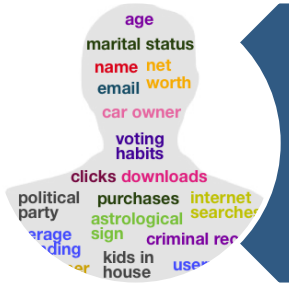
- Cash
- Check
- Debit
- Credit
- Prepaid
- Online banking bill pay
- Bank account number payment
- Money order

3 factors important for choice

1. Characteristics of the consumer
   - Income(individual and household)
   - Demographics
2. Characteristics of the transaction
   - Dollar value
   - Type of expenditure (bills, nonbills, P2P)
3. Characteristics of the payment instrument
   - Security
   - Cost
   - Convenience

Three kinds of security

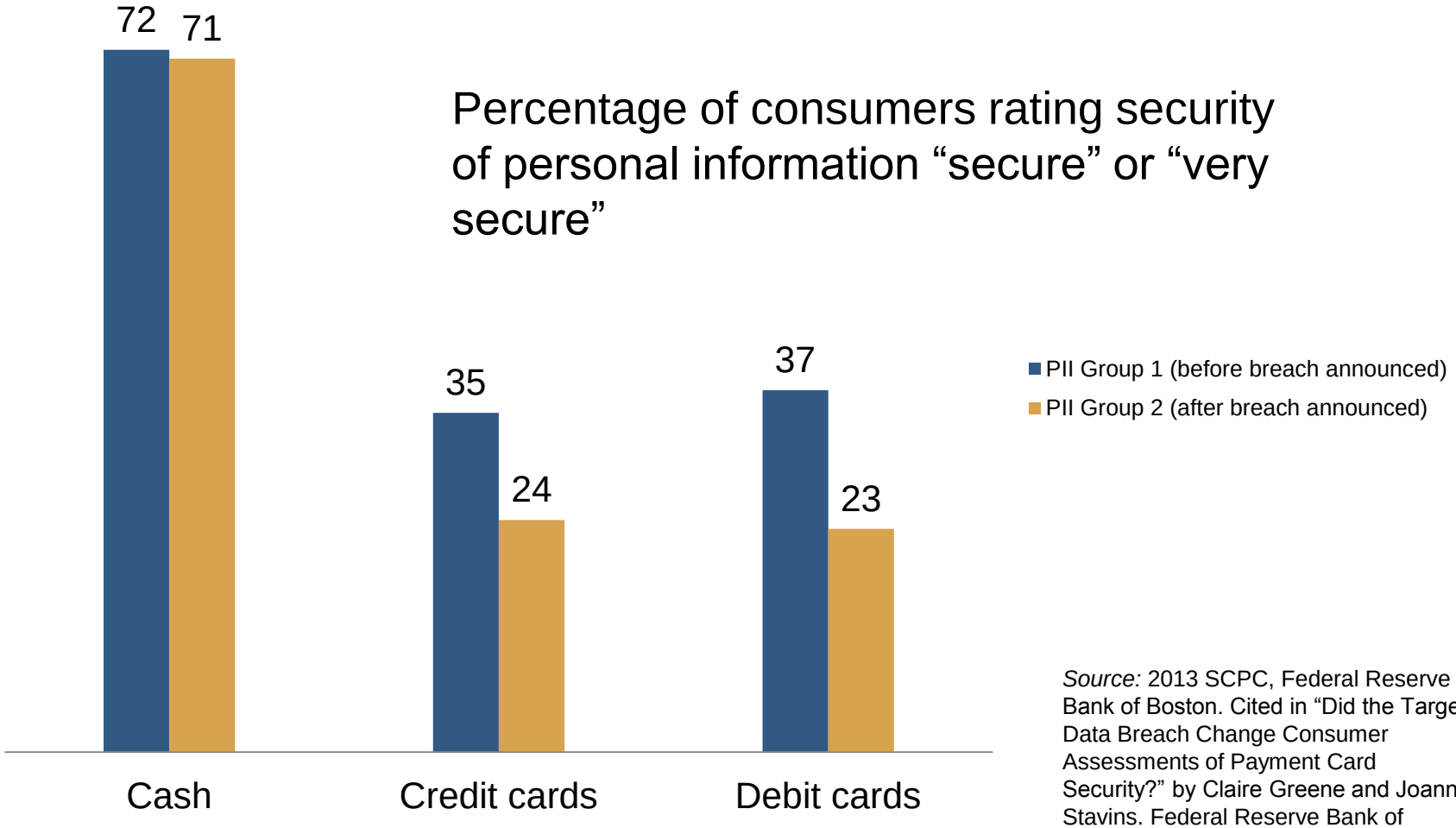
security of **wealth**



security of
personal info

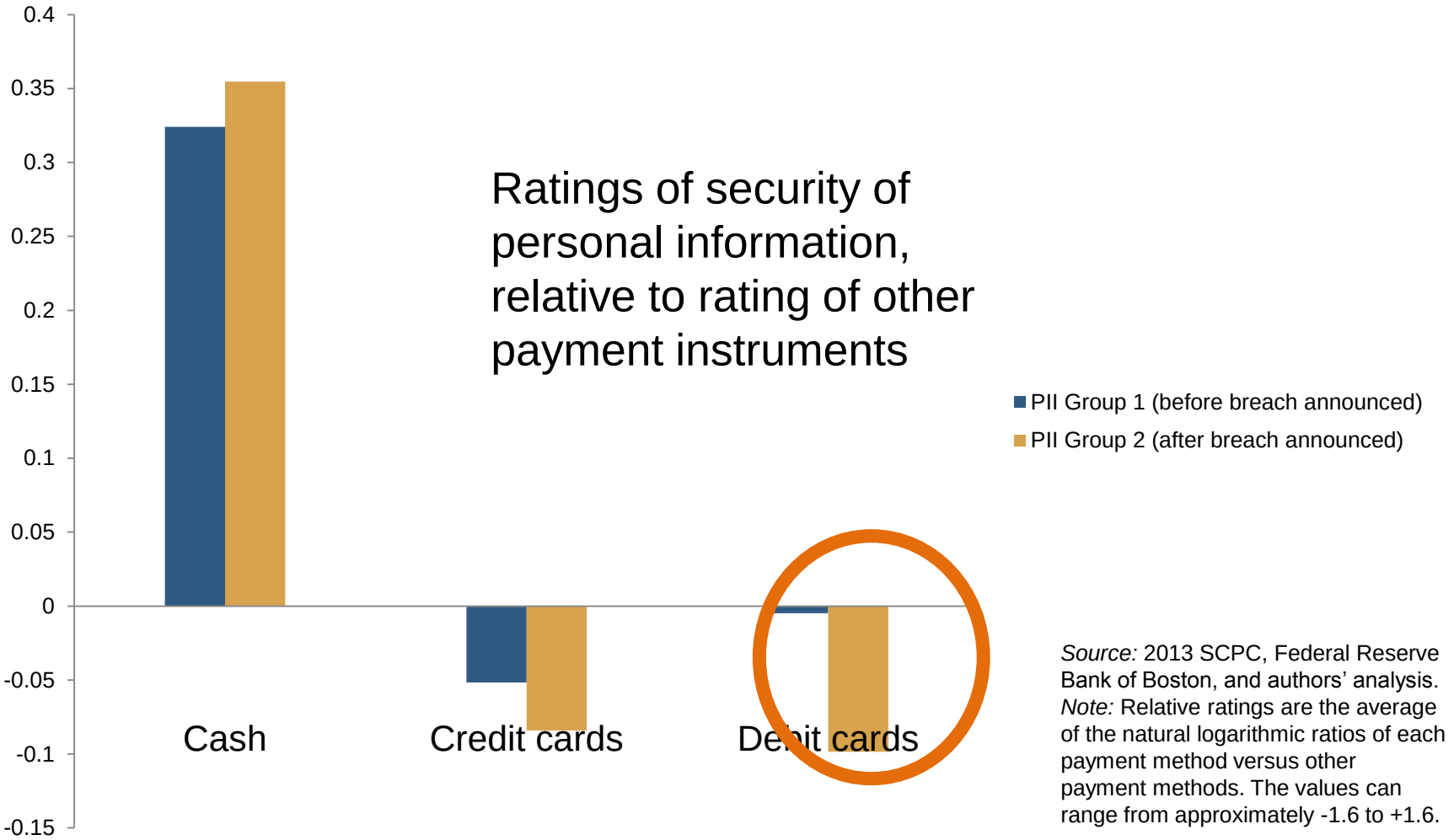
privacy of
transaction

Ratings of security of personal information



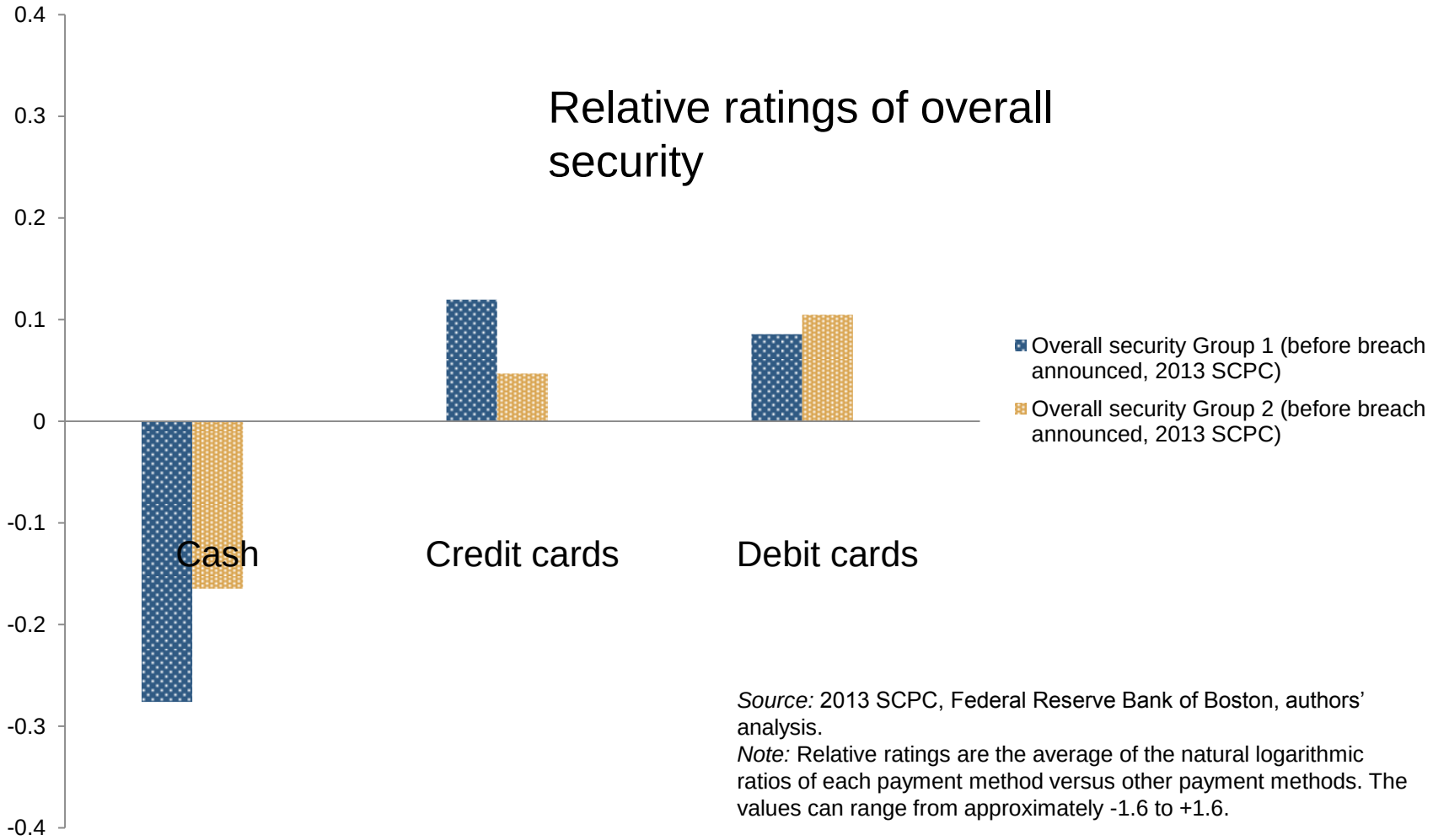
Source: 2013 SCPC, Federal Reserve Bank of Boston. Cited in “Did the Target Data Breach Change Consumer Assessments of Payment Card Security?” by Claire Greene and Joanna Stavins. Federal Reserve Bank of Boston Research Data Report 16-1.

Ratings relative to all payment methods



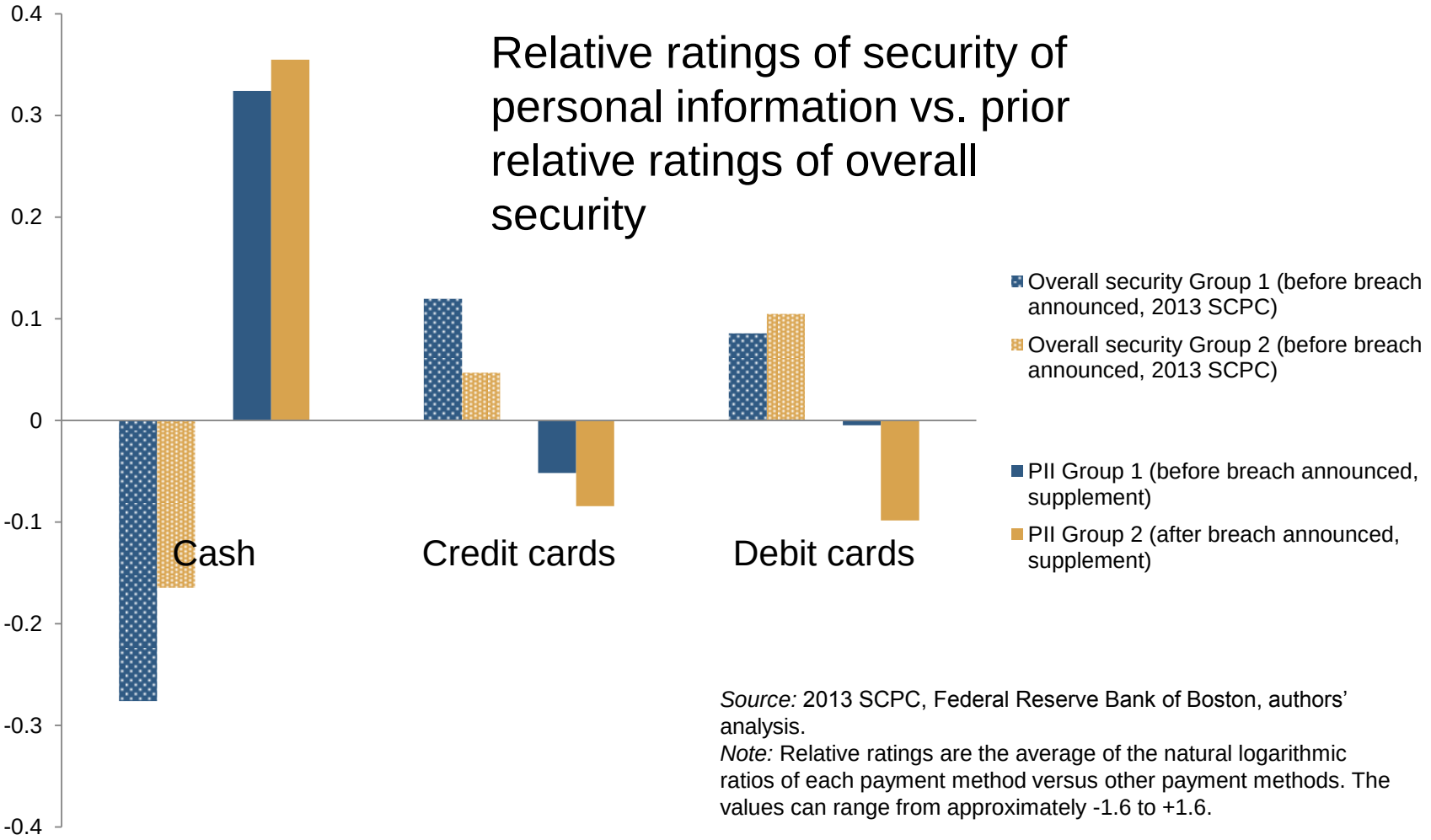
Source: 2013 SCPC, Federal Reserve Bank of Boston, and authors' analysis.
Note: Relative ratings are the average of the natural logarithmic ratios of each payment method versus other payment methods. The values can range from approximately -1.6 to +1.6.

Prior rating of “security”



Source: 2013 SCPC, Federal Reserve Bank of Boston, authors’ analysis.
Note: Relative ratings are the average of the natural logarithmic ratios of each payment method versus other payment methods. The values can range from approximately -1.6 to +1.6.

Comparison to prior rating of "security"



Source: 2013 SCPC, Federal Reserve Bank of Boston, authors' analysis.
Note: Relative ratings are the average of the natural logarithmic ratios of each payment method versus other payment methods. The values can range from approximately -1.6 to +1.6.

Debit rated poorly after a breach

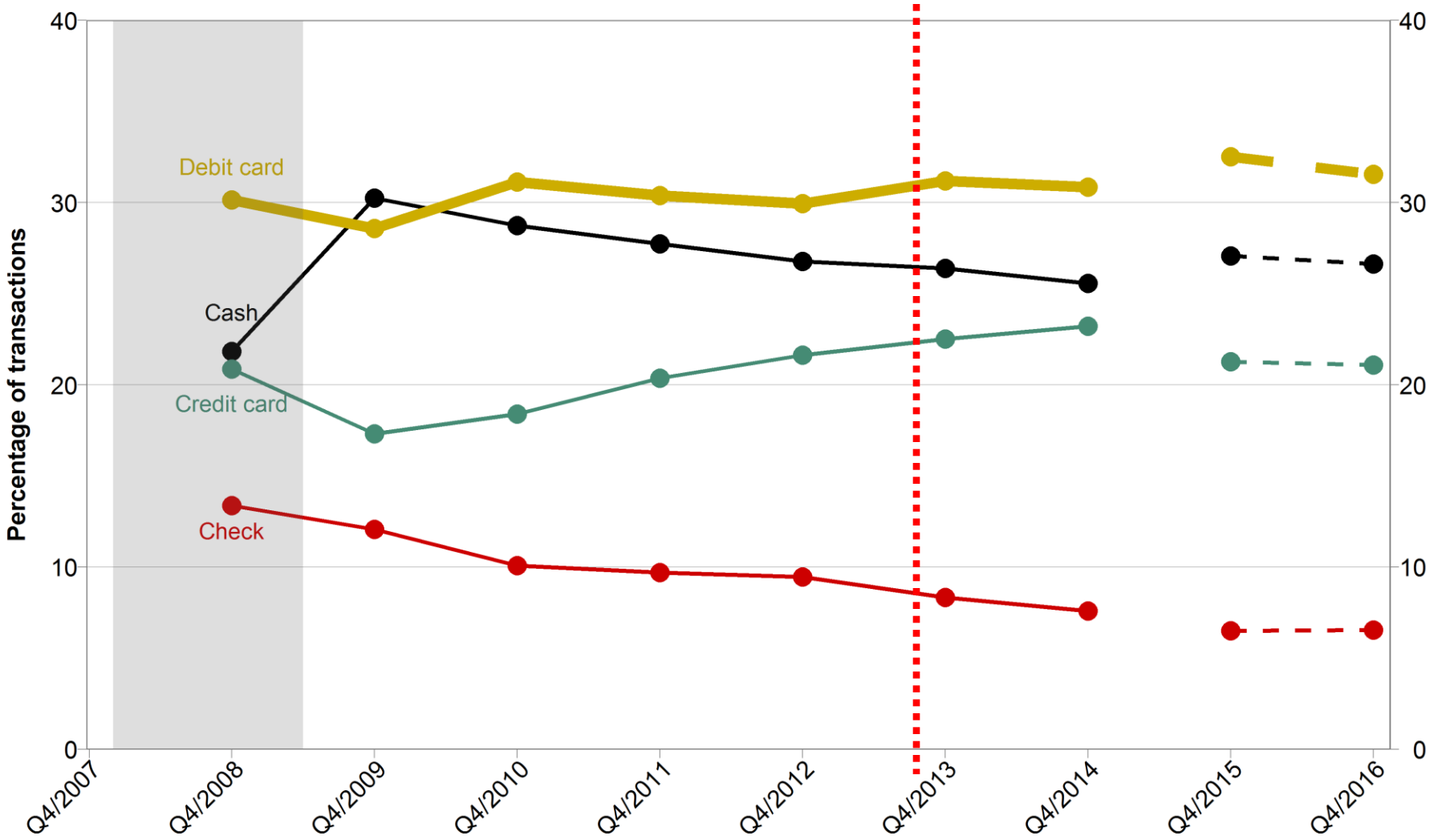
For security of personal info

after Target 2013 data breach

Relative to other payment instruments

Debit cards

No long-term effects observed

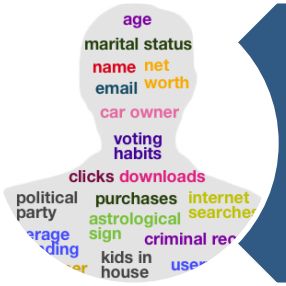


Source: Survey of Consumer Payment Choice.
2015 & 2016 results are preliminary and not official.

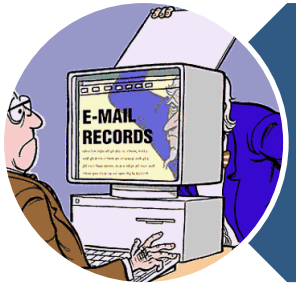
Would better security increase use?

For credit & debit cards, the economic effect is small

Small change: Increased security of wealth



No change: Increased security of personal info



No change: Increased privacy of transaction

Source: 2013 Survey of Consumer Payment Choice. Cited in "How Do Speed and Security Influence Consumers' Payment Behavior?" by Scott Schuh and Joanna Stavins forthcoming in *Contemporary Economic Policy.*

Research reports & data

- Reports, data tables, raw data for download
  - https://www.bostonfed.org/payment-studies-and-strategies.aspx
  - "Did the Target Data Breach Change Consumer Assessments of Payment Card Security?"
  - "How Do Speed and Security Influence Consumers' Payment Behavior?"

Thank you!

Claire Greene, payments analyst
Consumer Payments Research Center
Federal Reserve Bank of Boston
Claire.m.greene@bos.frb.org

CONSUMER PAYMENTS Research Center

FEDERAL RESERVE BANK OF BOSTON™

How Data Breaches Affect Consumer Credit[1]

NACHA PAYMENTS 2017

April 24, 2017

Slava Mikhed

Payment Cards Center
Federal Reserve Bank of Philadelphia

Michael Vogan

Moody's Analytics

[1] The views expressed here are those of the speaker and not necessarily those of the Federal Reserve Bank of Philadelphia, the Federal Reserve System, or Moody's Analytics. No statements here should be treated as legal advice.

FEDERAL RESERVE BANK OF PHILADELPHIA

South Carolina Department of Revenue Breach

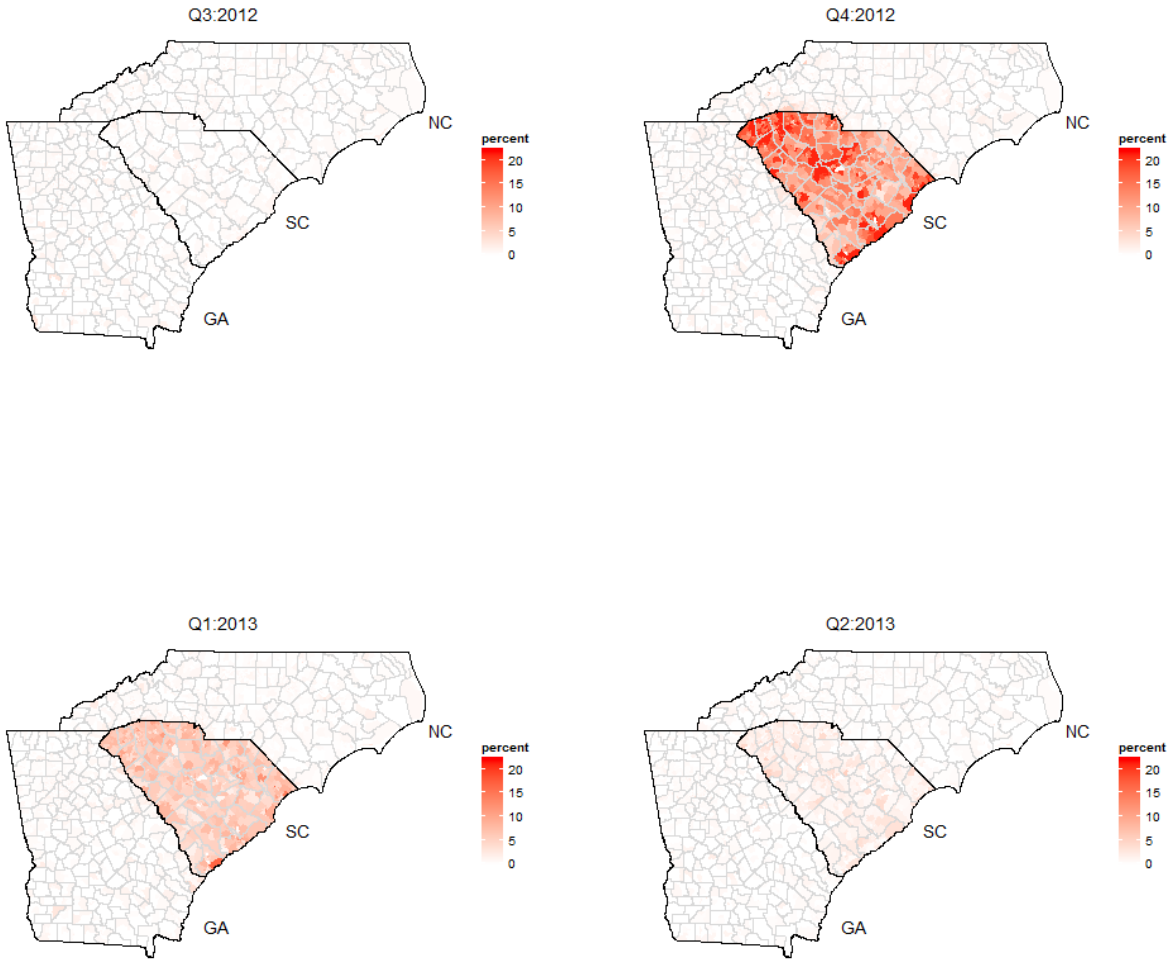
- Publicly announced on October 26, 2012
  - 81% SC residents affected
  - Very few SC non-residents affected
  - Payment and bank info stolen
  - Social Security numbers stolen
  - Addresses, names, birth dates stolen

- We study how victims reacted
- Use FRBNY Consumer Credit Panel / Equifax data

Focus on 4 Fraud Protection Services

- Initial Alerts
  - Free service that expires after 90 days
  - Lenders must apply reasonable policies and practices to verify applicant's identity
- Freezes
  - Block all access to credit files
  - May impose initiation / removal fee
- Opt-outs
  - Free removal from prescreened solicitation lists
- Credit Watches
  - Commercial, fee-based services that may provide one or a combination of credit monitoring, unlimited credit report access, and fraud insurance

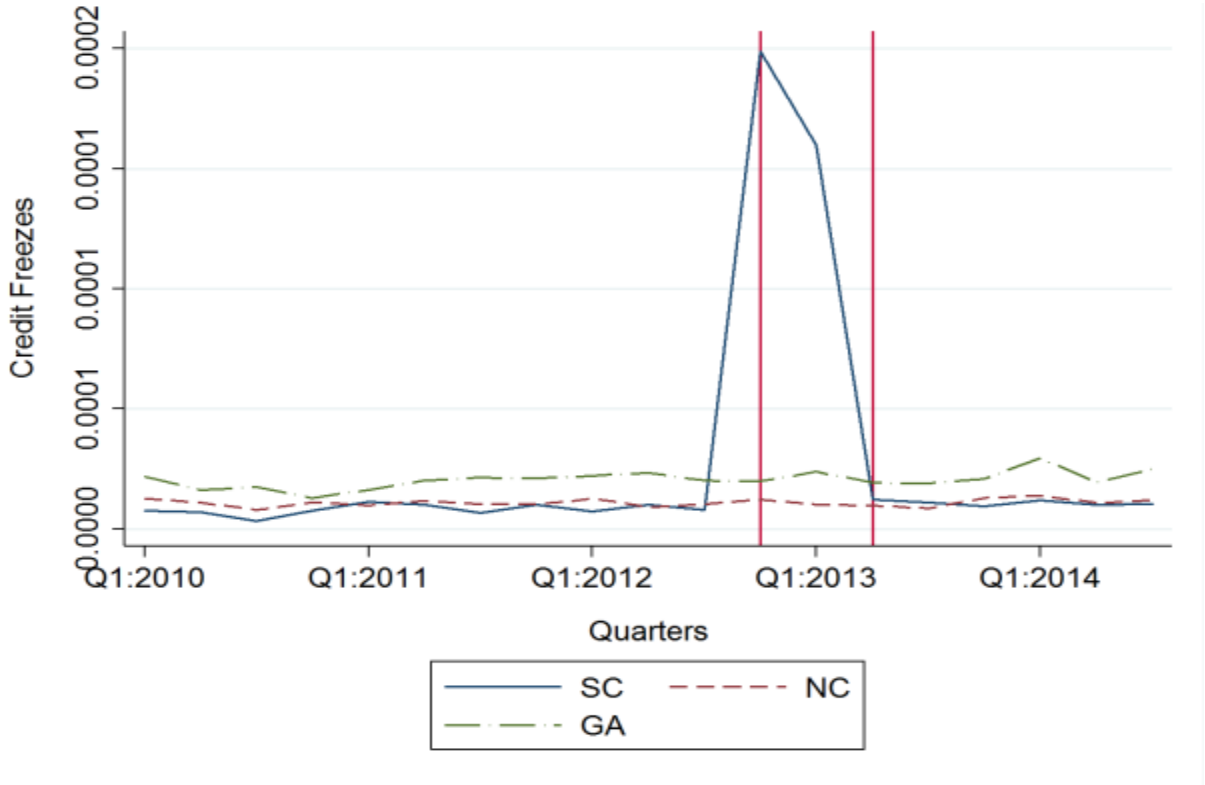
Breach Increases Quarterly Fraud Protection Take-up in SC only (Share of Population)



Note: Based on authors' calculations using data from 2010 Census and the FRBNY CCP / Equifax, augmented with variables acquired by the Payment Cards Center

Methodology: Difference-in-Differences on SC vs. NC and GA

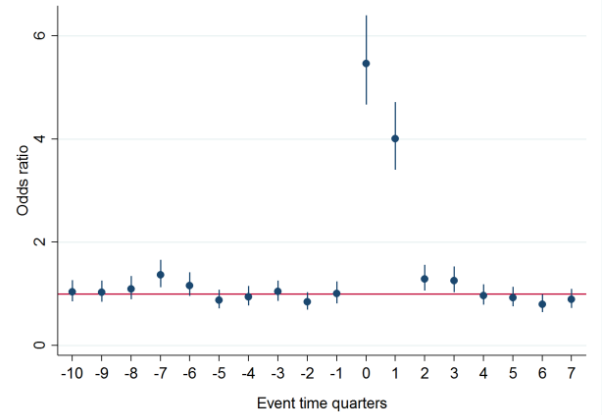
Parallel trends up to the time of the breach



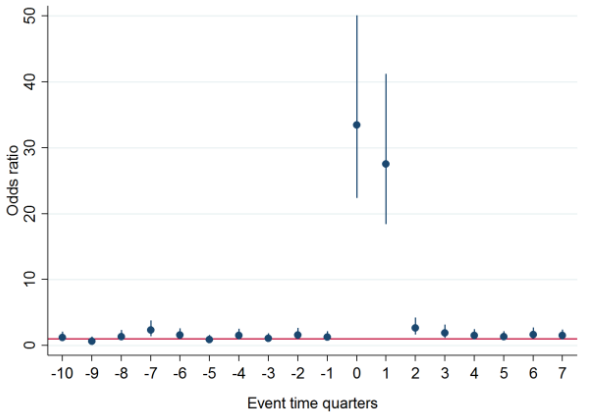
Source: Authors' calculations using data from the FRBNY CCP / Equifax, augmented with variables acquired by the Payment Cards Center

Take-up of Protection Spikes

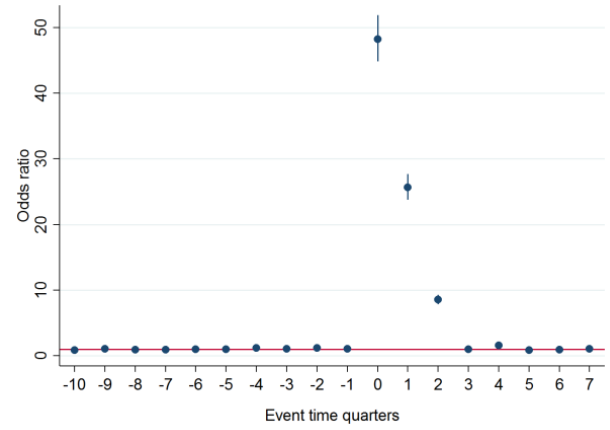
Panel A: Initial Alerts



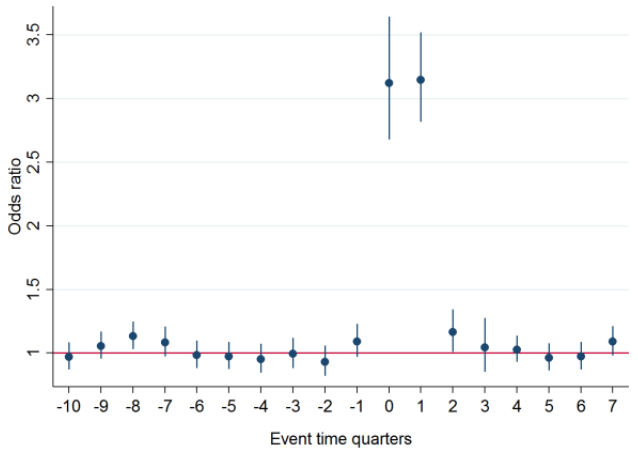
Panel B: Credit Freezes



Panel C: Credit Watches



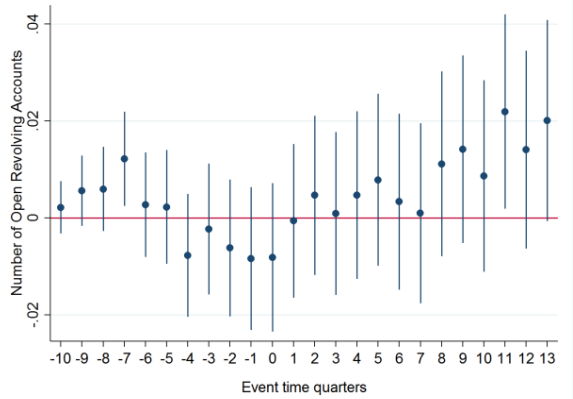
Panel D: Opt-outs



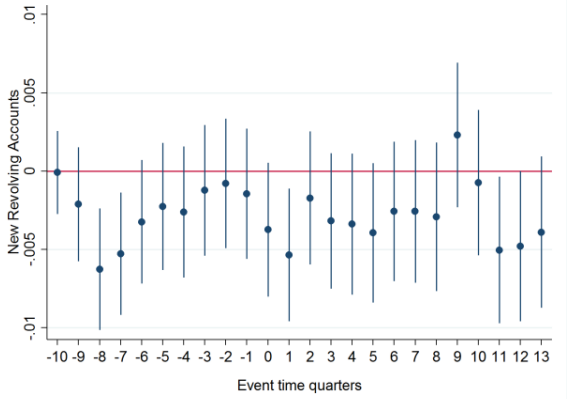
Notes: Authors' calculations using data from the FRBNY CCP / Equifax, augmented with variables acquired by the Payment Cards Center. An odds ratio is the ratio of the probabilities of filing and not filing for protection.

No Response on Credit Card Usage

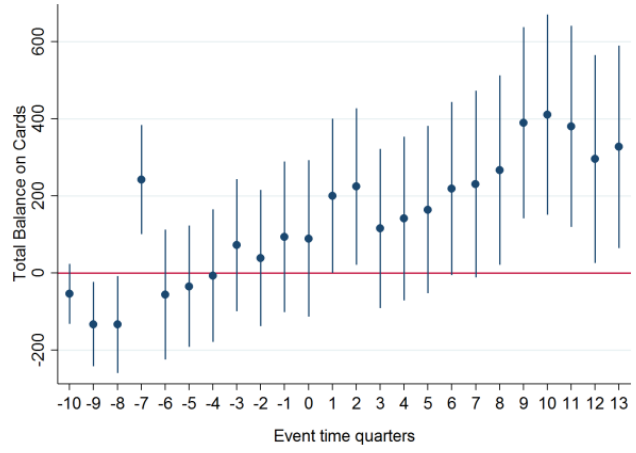
Panel A: Number of Open Cards



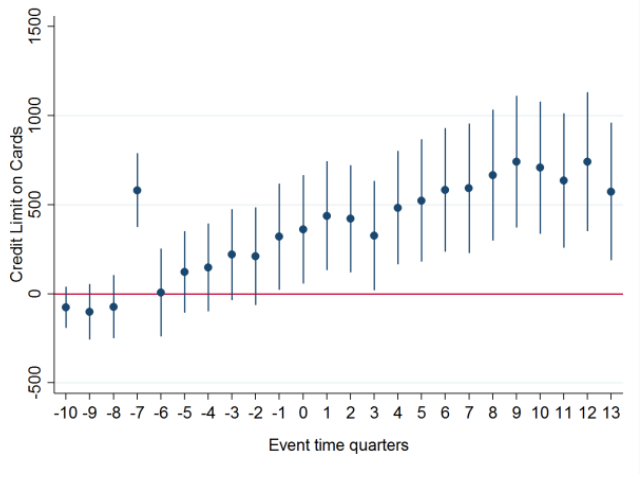
Panel B: New Cards



Panel C: Total Card Balance



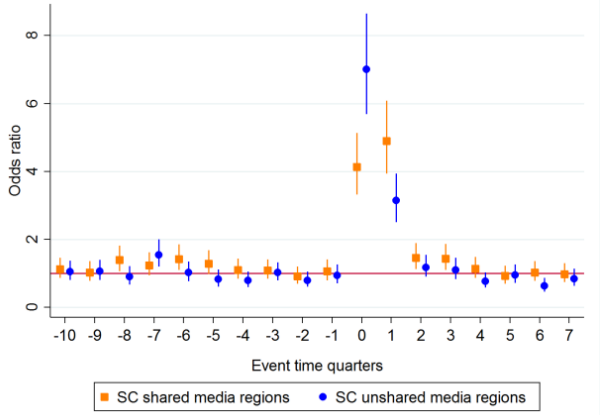
Panel D: Credit Card Limits



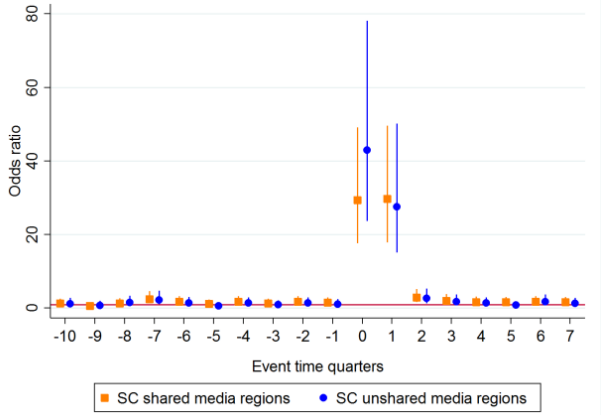
Notes: Authors' calculations using data from the FRBNY CCP / Equifax, augmented with variables acquired by the Payment Cards Center.

Receiving “Diluted” News Reduced Take-Up a Bit

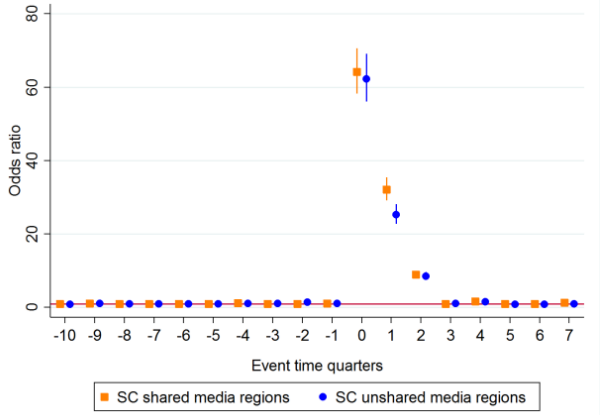
Panel A: Initial Alerts



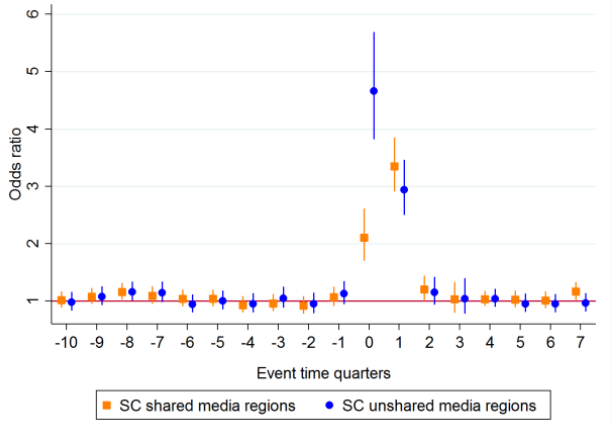
Panel B: Credit Freezes



Panel C: Credit Watches



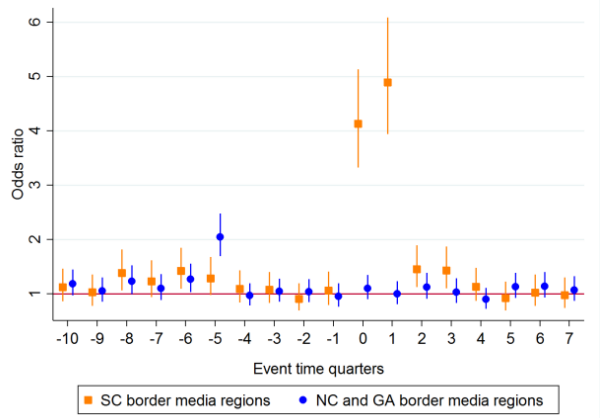
Panel D: Opt-outs



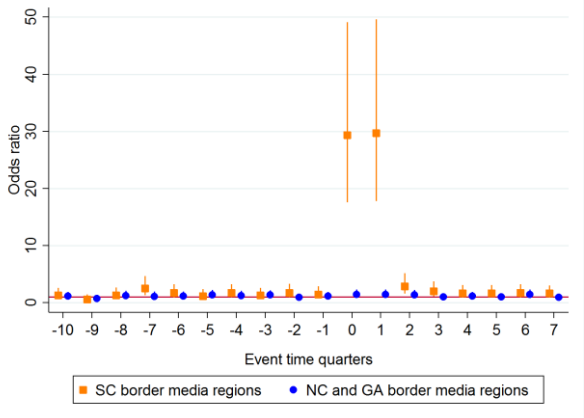
Source: Authors’ calculations using data from the FRBNY CCP / Equifax, augmented with variables acquired by the Payment Cards Center

No Effect of News on Non-victims (NC or GA)

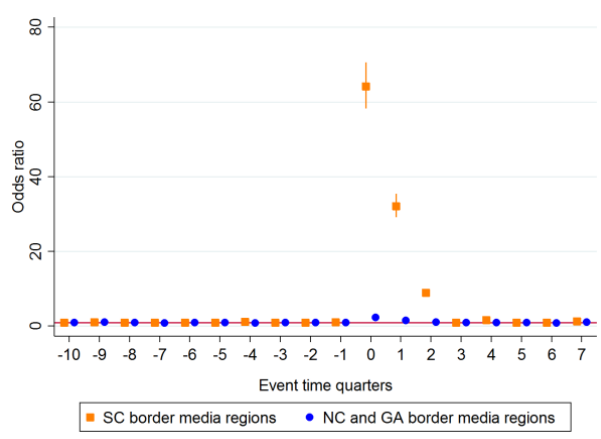
Panel A: Initial Alerts



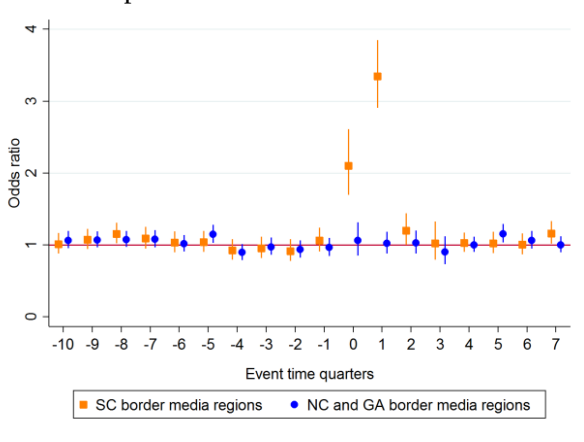
Panel B: Credit Freezes



Panel C: Credit Watches



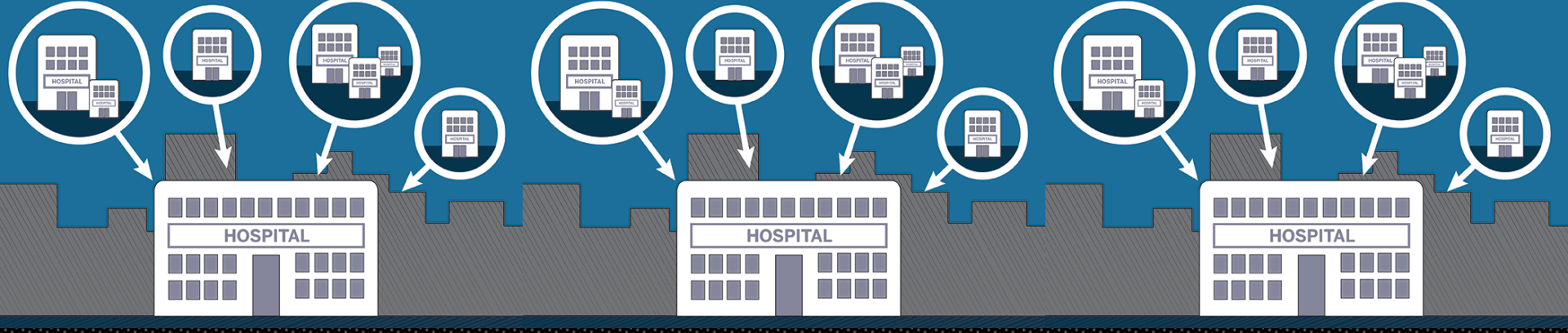
Panel D: Opt-outs



Source: Authors' calculations using data from the FRBNY CCP / Equifax, augmented with variables acquired by the Payment Cards Center

Summary

- SC breach induced consumers to get fraud protections
- Breach notifications may help consumers protect against ID theft
- Breach victims continued their normal use of credit cards and credit
- No effect of the breach or news about it on non-victims outside of SC
- Consumers appear very confident in the payment card systems



Do Patients Care about Data Breaches?

M. Eric Johnson

Juhee Kwon

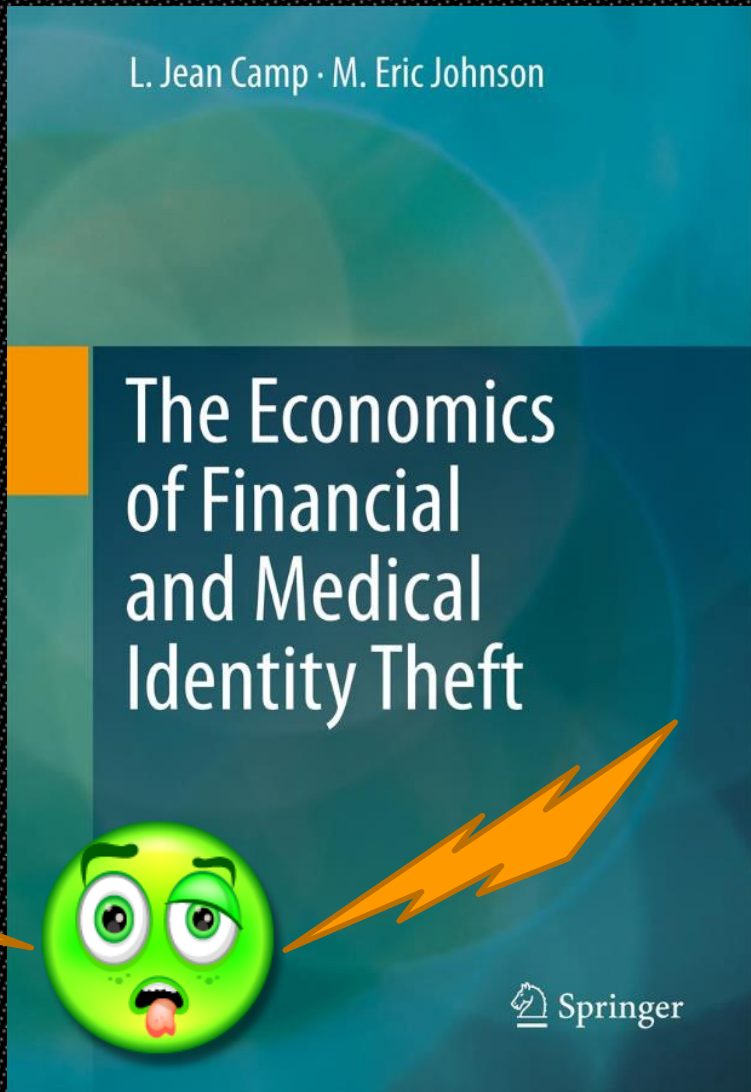
VANDERBILT UNIVERSITY
OWEN GRADUATE SCHOOL OF MANAGEMENT

Two Sides to Security Economics

- Patients: Economics of fraud and harm.
- Organizations: Economics of security investment and cost of security failures.

Medical Fraud Models

- Don’t know the first digit - but $100’s of billions on US $2.5T spend
- Involving Stolen/Misused Identities
  - False service claims
  - Drugs, equipment, and supplies (false claims, diluting medication, etc)
  - Identity trafficking
- Other
  - Patient participation (e.g., false claims, sharing, equipment)
  - Unnecessary testing and treatment
  - Kickbacks
  - Referrals (self and others with financial entanglement)
  - Pricing
  - Illegal distribution of controlled substance
  - Embezzlement



Cost to Providers

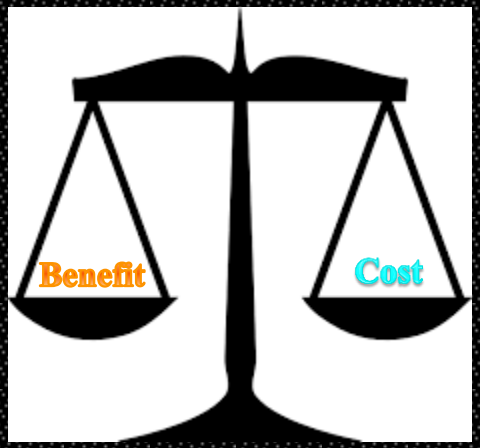
- Hold-ups
- Brand damage
- Liability
- Disclosure

Economic Drivers for Firms

- Problem: Costs have impacted patients (and payers) more than providers. Market Failure – under investment.
- Problem: Patients can't evaluate security effort. Information asymmetry - under investment.
  - How to solve?

Government Intervention

The U.S. government has been working to make the cost and benefit of security more apparent by imposing breach notification, monetary incentives, and penalties.



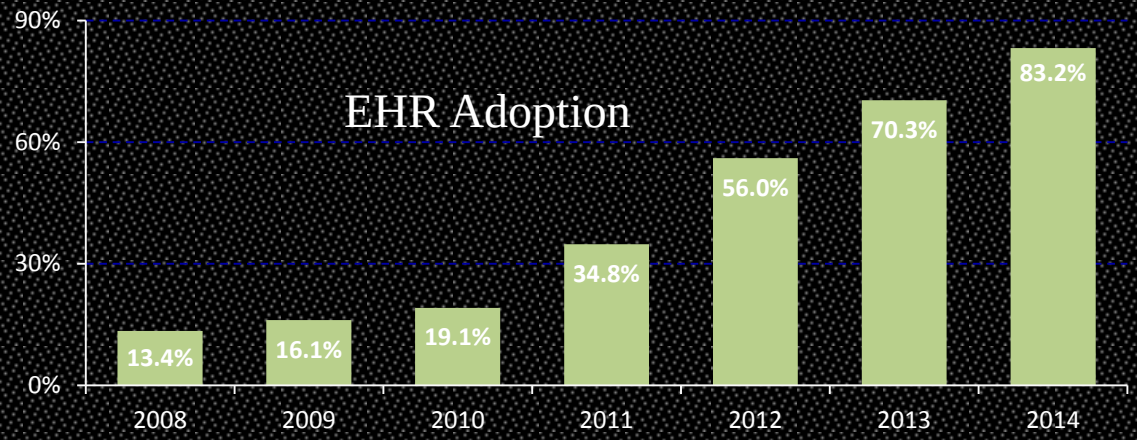
Regulatory Intervention

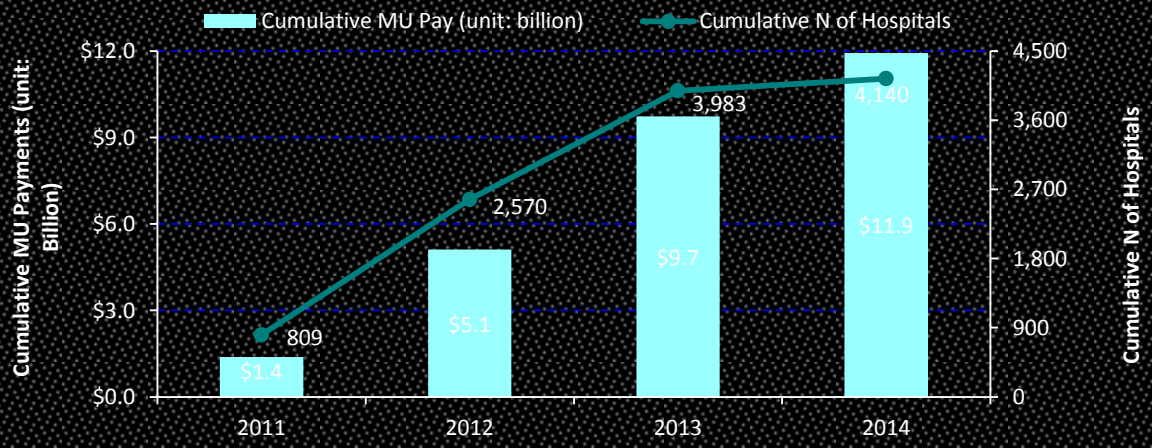
(breach notification, incentives, and penalties)

Government Tinkering

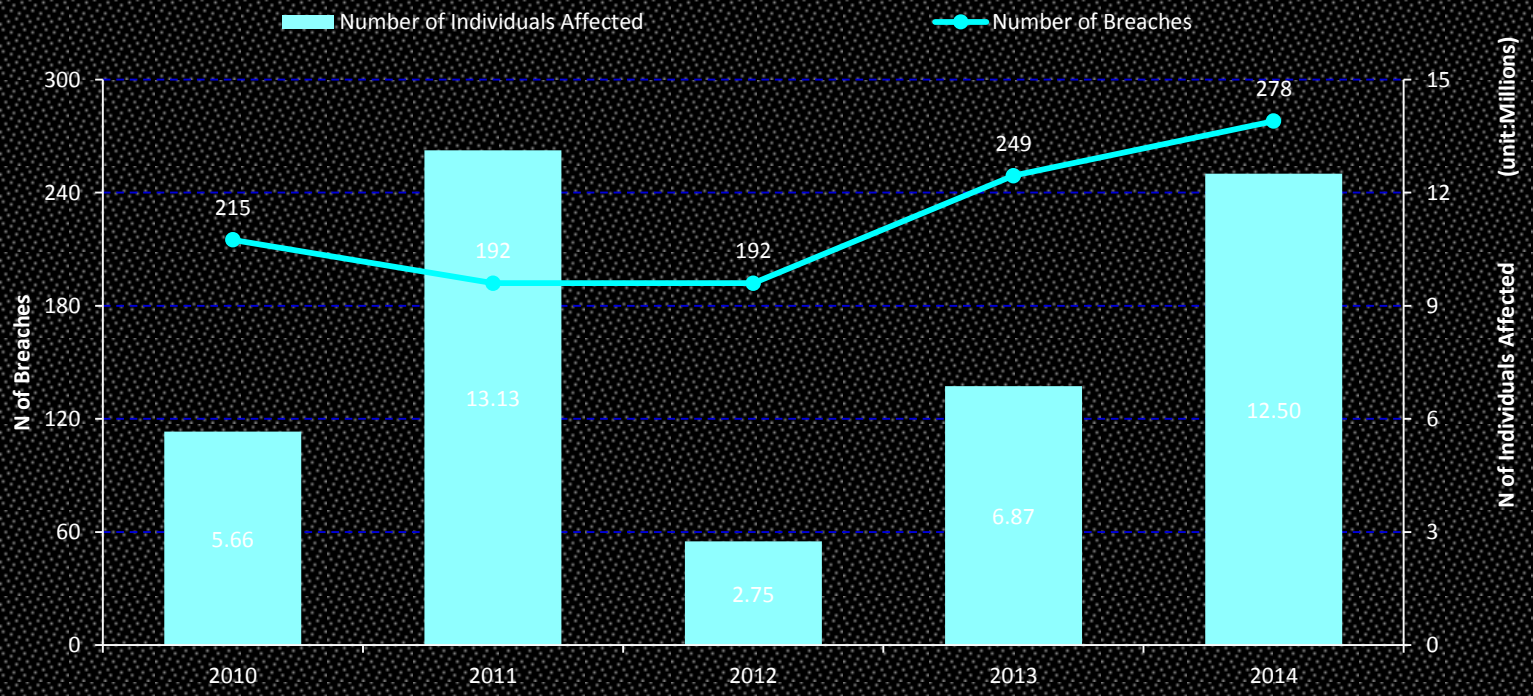
- **Incentives to Invest (proactive is best).**
- Costs for failures (it works).
  - Penalties
  - Breach disclosure (cost to disclose)
- Reduce information asymmetry (it works).
  - Disclosure -> market pressure.

HITECH – Follow the $





Breaches


Number of Individuals Affected
Number of Breaches
N of Breaches
N of Individuals Affected (unit:Millions)
300
240
180
120
60
0
15
12
9
6
3
0
215
192
192
249
278
5.66
13.13
2.75
6.87
12.50
2010
2011
2012
2013
2014

Government Tinkering

- Incentives to Invest (proactive is best).
- **Costs for failures (it works).**
  - Penalties
  - Breach disclosure (cost to disclose)
  - Liability?
- Reduce information asymmetry (it works).
  - Disclosure -> market pressure.

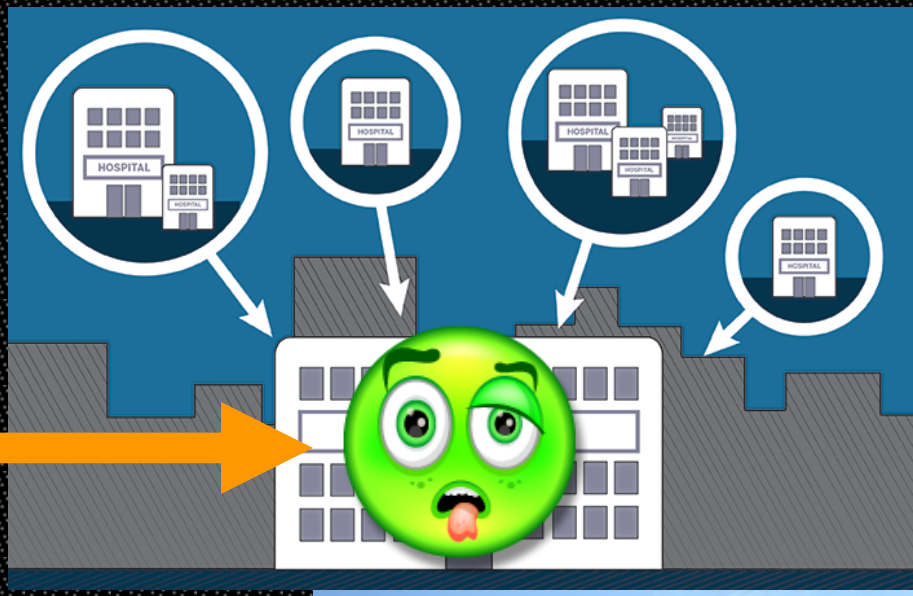
Government Tinkering

- Incentives to Invest (proactive is best).
- Costs for failures (it works).
  - Penalties
  - Breach disclosure (cost to disclose)
  - Liability?
- **Reduce information asymmetry (it works).**
  - Disclosure -> market pressure.

Media Coverage of Healthcare Breaches

- The HITECH Act requires hospitals to post their breaches on the Wall of Shame (The US Health & Human Services- HHS).
- The increased visibility of data breaches due to the HITECH Act.
  - Healthcare breaches have received significant media attention and public concern. For example, Anthem received multi-day coverage for a breach affecting 80 million individuals.

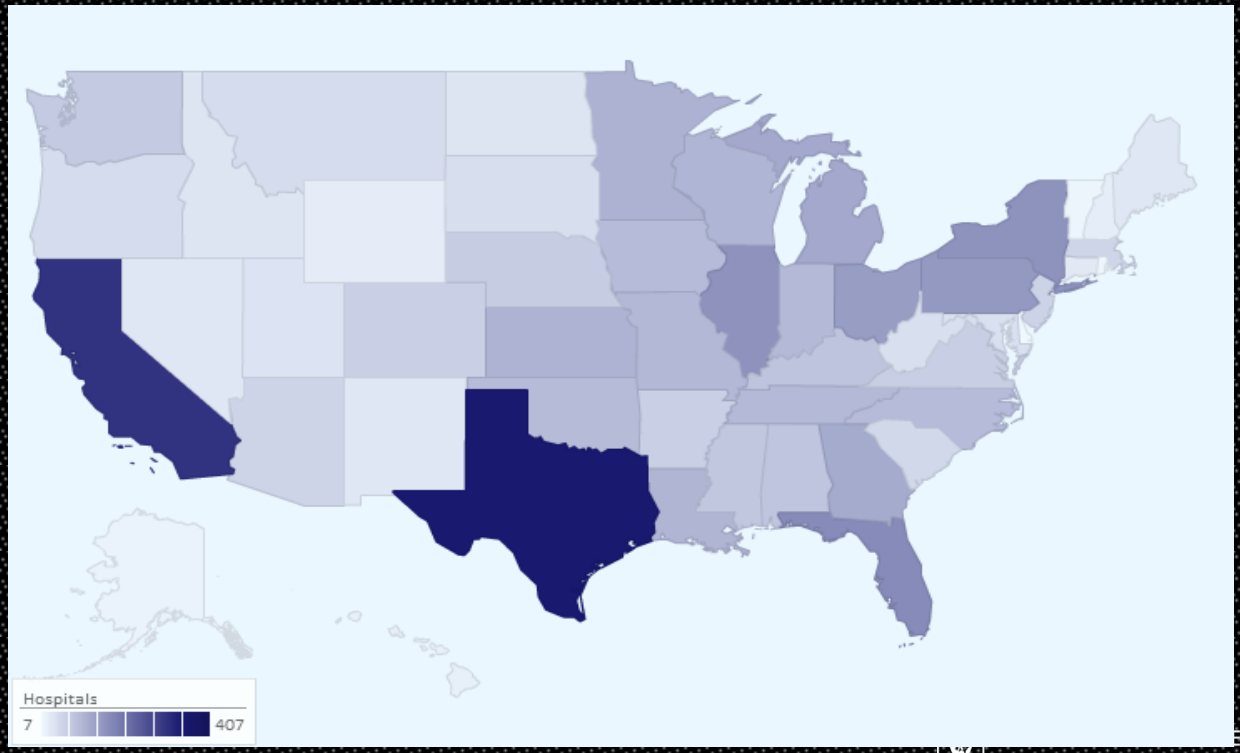
Competition



Data: Hospitals

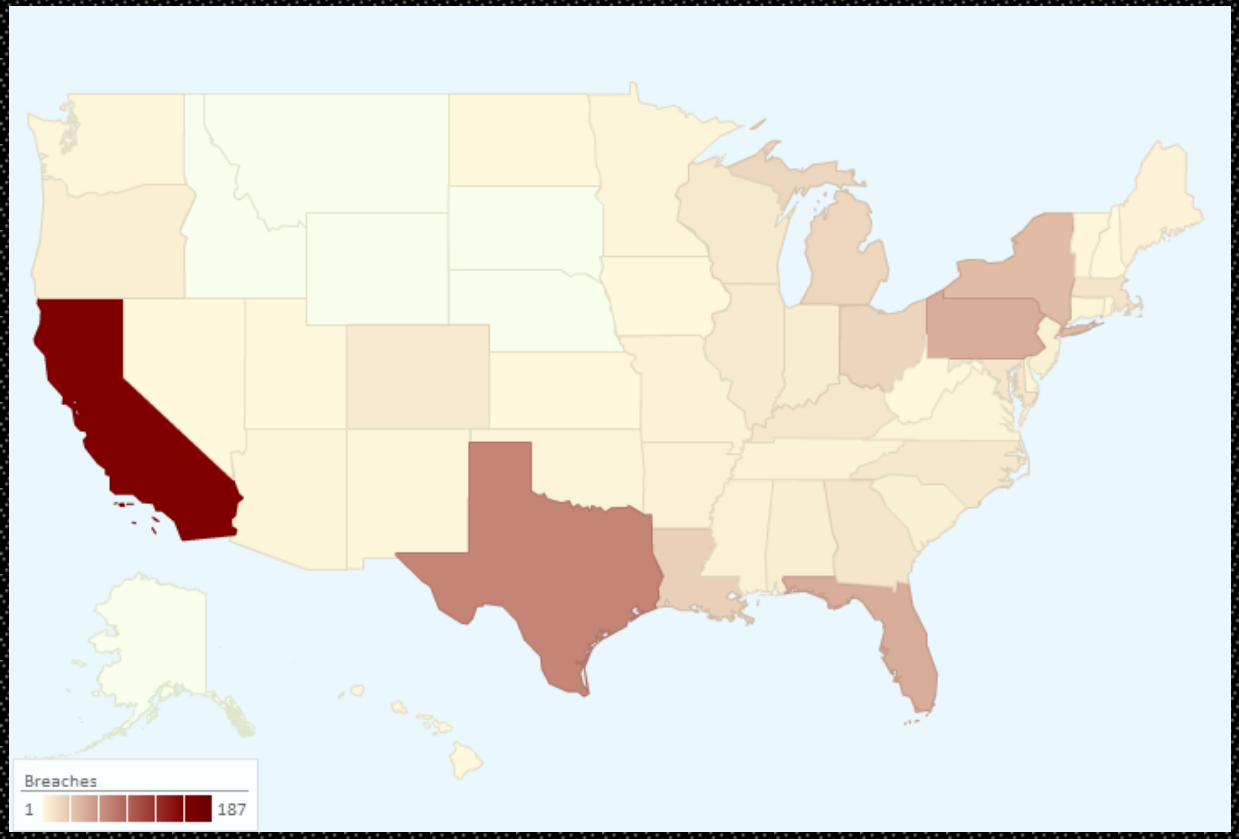
- Hospital information provided by HIMSS Analytics™ Database
  - 4,878 hospitals : admissions, outpatient visits, adopted healthcare and security applications, and organizational characteristics (i.e., operating expense, organizational type, bed size, academic, etc.).

State	#Hospitals
TX	407
CA	362
FL	202
IL	189
NY	188
…	…
VT	14
RI	11
DC	10
DE	7



Data: Breaches

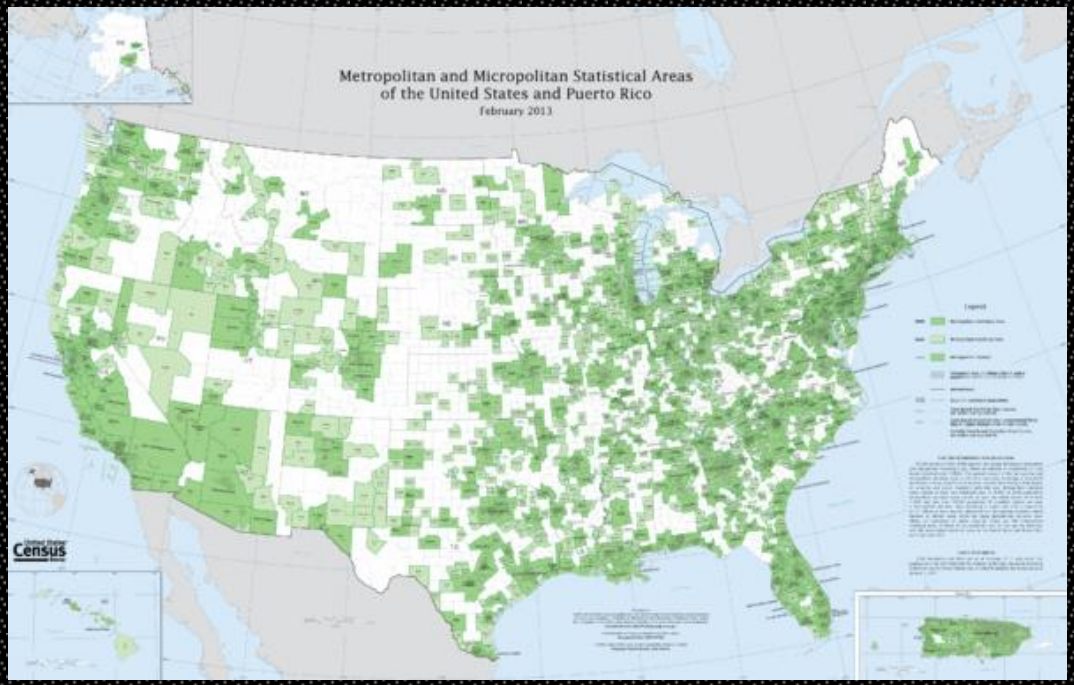
- **723 healthcare breaches from HHS and Privacy Clearinghouse.**



State	Breaches
CA	187
TX	87
PA	57
FL	57
NY	46
…	…
MT	0
WY	0

Data: Healthcare Market

- The Area Health Resources Files (AHRF) - http://ahrf.hrsa.gov/
  - Total population, the population eligible for Medicare, and the number of hospitals at the Core Based Statistical Area (CBSA) level.
    - A CBSA is a U.S. geographic area of at least 10,000 people and adjacent areas.



Finding: Breaches impact patients

- **Admissions trends between the pre and post-breach periods in treatment hospitals dropped by 30.6%**
- **Outpatient-visit trends between the pre- and post-breach periods in treatment hospitals saw reductions of 32.6%**

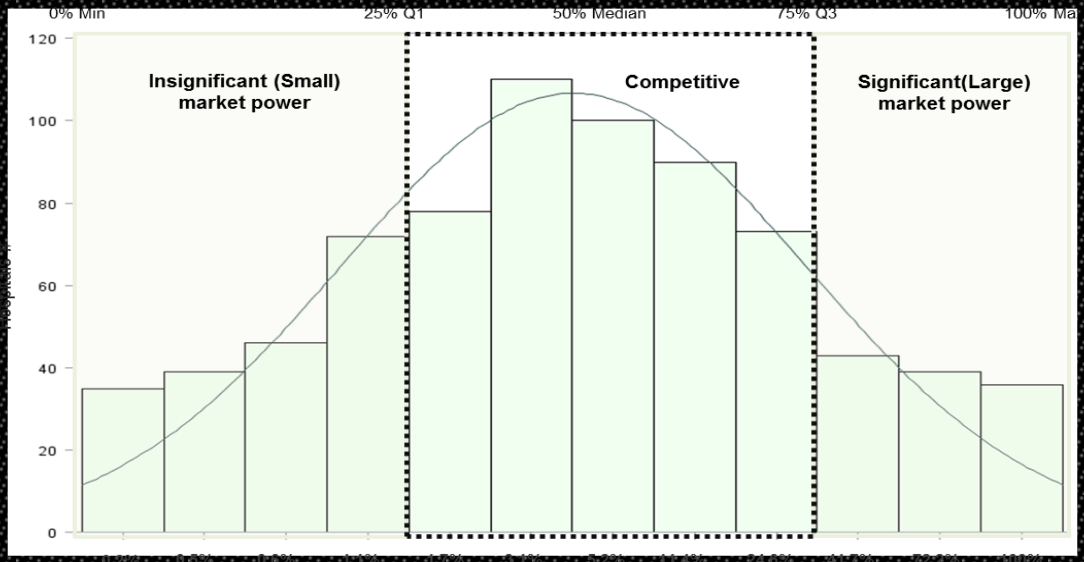
So a hospital growing by 10% would see only 7% growth.

Finding: Timing and Size Matter

- Single breaches have no short-term impact on either admissions or outpatient visits.
- The cumulative effect of multiple data breaches over 3 year is associated with a significant decrease in both admissions and outpatient visits.
- Larger breaches are associated with larger decreases in admissions and outpatient visits.

Finding: Market Power Matters

- Healthcare markets exhibit geographical-based competition within each local area.
  - We categorized hospitals into three groups based on their market share.



No impact in uncompetitive markets

Hospitals facing competitive markets saw nearly double the effect