Should Credit Card Issuers Reissue Cards After a Data Breach?

Jim Graves, Alessandro Acquisti, Nicolas Christin
Carnegie Mellon University

Issuer Options Post-Breach

- When a credit card is compromised in a breach, issuers can recover "fraud losses" from an merchant's acquiring bank but not "operational costs."
- The law expects plaintiffs to mitigate damages
- Issuer choices:
  - Reissue all cards; possibly without reimbursement
  - Wait and see; may not have mitigated damages

Research Question

- Which option has the lowest societal cost?

Challenges

- Poor data
  - What is the likelihood that a card affected in a breach will be used for fraud?
  - How many credit cards are affected in breaches?
  - How much credit card fraud is due to breach?

Research Approach

- Cost-benefit estimation
  - Ranges
  - Monte Carlo analysis
- Focued primarily on direct costs

Cost of Reissuing Cards

- $3–$25
  - Based on claims in lawsuits and figures quoted in news articles
- Economies of scale seem to apply

Source	Cards	$/Card
Pa. State Empl. Credit Union[1]	20,000	$5
Fulton Bank[2]	20,000	$5
Sovereign Bank[3]	81,000	$6
Merrill Bank[4]	71	$14
TrustCo Bank[5]	4,000	$20

[1] Pa. State Employees Credit Union v. Fifth Third Bank, 398 F. Supp. 2d 317, 321 (M.D. Pa. 2005).
[2] Eric Stark, *Computer Hackers are Stealing Bank Card Information, but There Is Protection and Some Banks Have Been Aggressive*, Sunday News (Lancaster, Pa.), July 11, 2004, at 1
[3] Mark Jewell, *IDs Are a Steal*, Columbian (Vancouver, WA), Aug. 23, 2004, at E
[4] Ann Ravana, *Banks Start Credit Card Reissue*, Bangor Daily News, Feb. 8, 2007, at 4
[5] Chris Churchill, *TJX Reacts to Bank Lawsuit*, Times Union (Albany, N.Y.), Aug. 30, 2008.

Cost of Not Reissuing Cards

- Expected cost of fraudulent use
  - Cost of fraud
  - Probability of misuse
- Easy to calculate with the right data
- We do not have the right data
- But maybe we can estimate with data we have?

Estimating the Cost of Not Reissuing Cards

- Can estimate based on
  - Number of credit card accounts breached (and not reissued) per year
  - Number of credit card fraud incidents per year
  - Percentage of those incidents in which card information was obtained via breach

Estimating the Cost of Not Reissuing Cards

- These data sources also have problems!
- (But at least the data exist.)

Data Issues

- Cards vs. accounts vs. households
- How many breached credit card accounts?
- How much card fraud is because of breach?
- How effective is fraud monitoring at reducing fraud?

Cards, Accounts, or Households

- Cards per account: ~1.2; accounts per household: ~6–9
  - Nilson Report, Statistical Abstract, Fed. Reserve Bank of NY

How Many Breached Credit Cards?

- Disclosed breaches
- Known but undisclosed breaches
- Undetected breaches

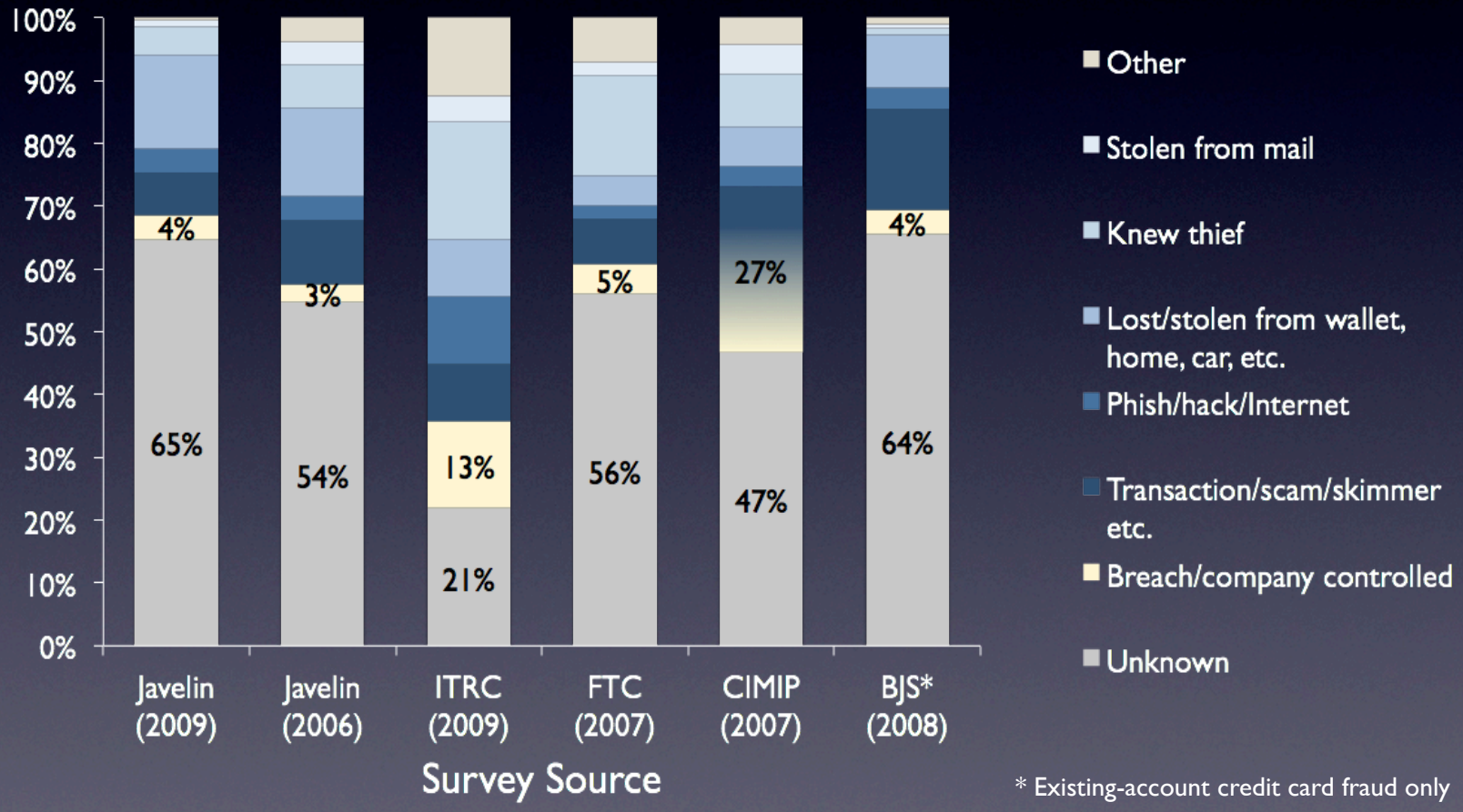
Estimating the Number of Breached Credit Cards

- Manually extracted from PRC database breaches affecting credit cards
- Ranges for disclosed breaches with record counts
- Extrapolation to disclosed breaches without record counts
  - Weighted by breach type (hack, lost media, etc.)

Estimated Number of Cards Exposed in Breaches per Year (000s)

Description	Low	Point	High
Reported w/ record counts	35,000	38,000	41,000
Credit cards as percentage of breached payment cards	66%	72%	78%
Credit card numbers reported lost in breaches per year	23,100	27,400	32,000
Est. records per year in breaches with unknown record counts	150	2,900	7,500
Scaling factor for unreported or undetected breaches	1	1.34	2
Portion of breached cards reissued	0.90	0.78	0.60
Total	2,460	12,000	40,600

How Much Credit Card Fraud is Because of Breach?



* Existing-account credit card fraud only

How Effective is Fraud Monitoring at Reducing Fraud?

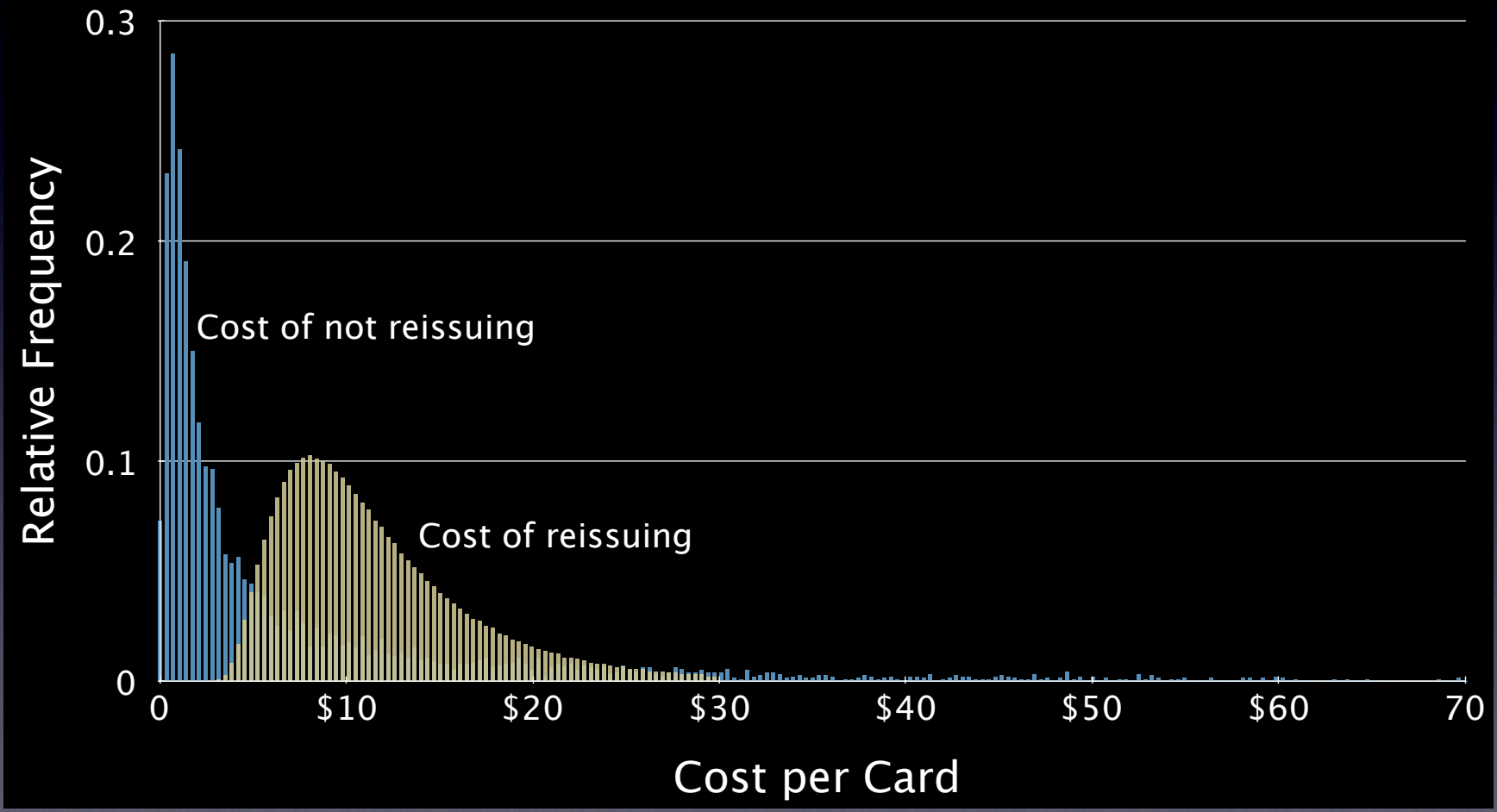
?

Expected Per-Card Cost of Not Reissuing Credit Cards

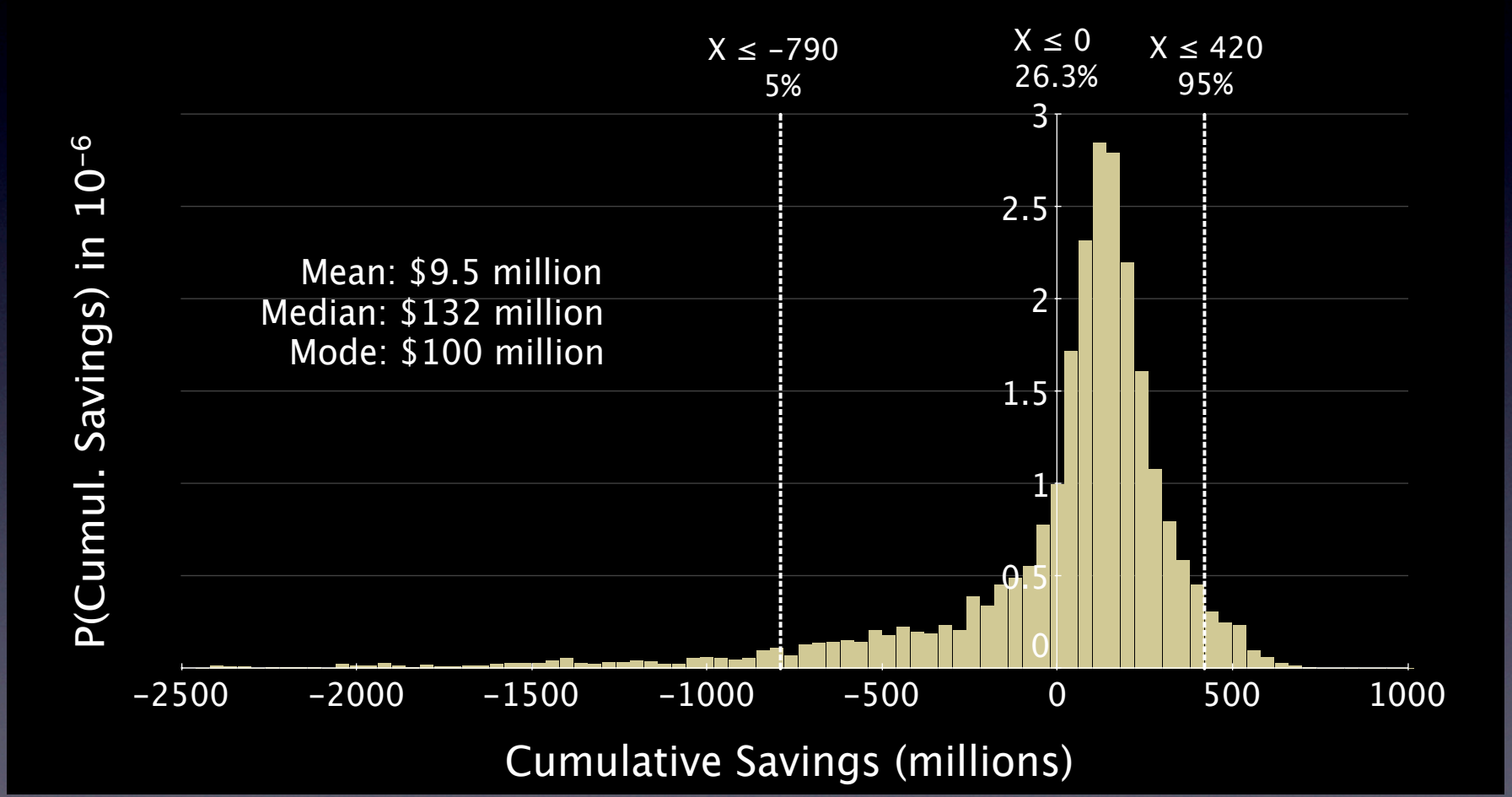
Description	Low	Point	High
P(EACCF | breach) ($\rho_{k,0}$)	0.0005	0.0056	0.0605
Cost of EACCF ($f_{k,0}$)	$1,000	$1,366	$1,500
Fraud reduction from flagging exposed cards	0%	10%	20%
Expected cost per card of not reissuing	$0.41	$7.50	$109.00

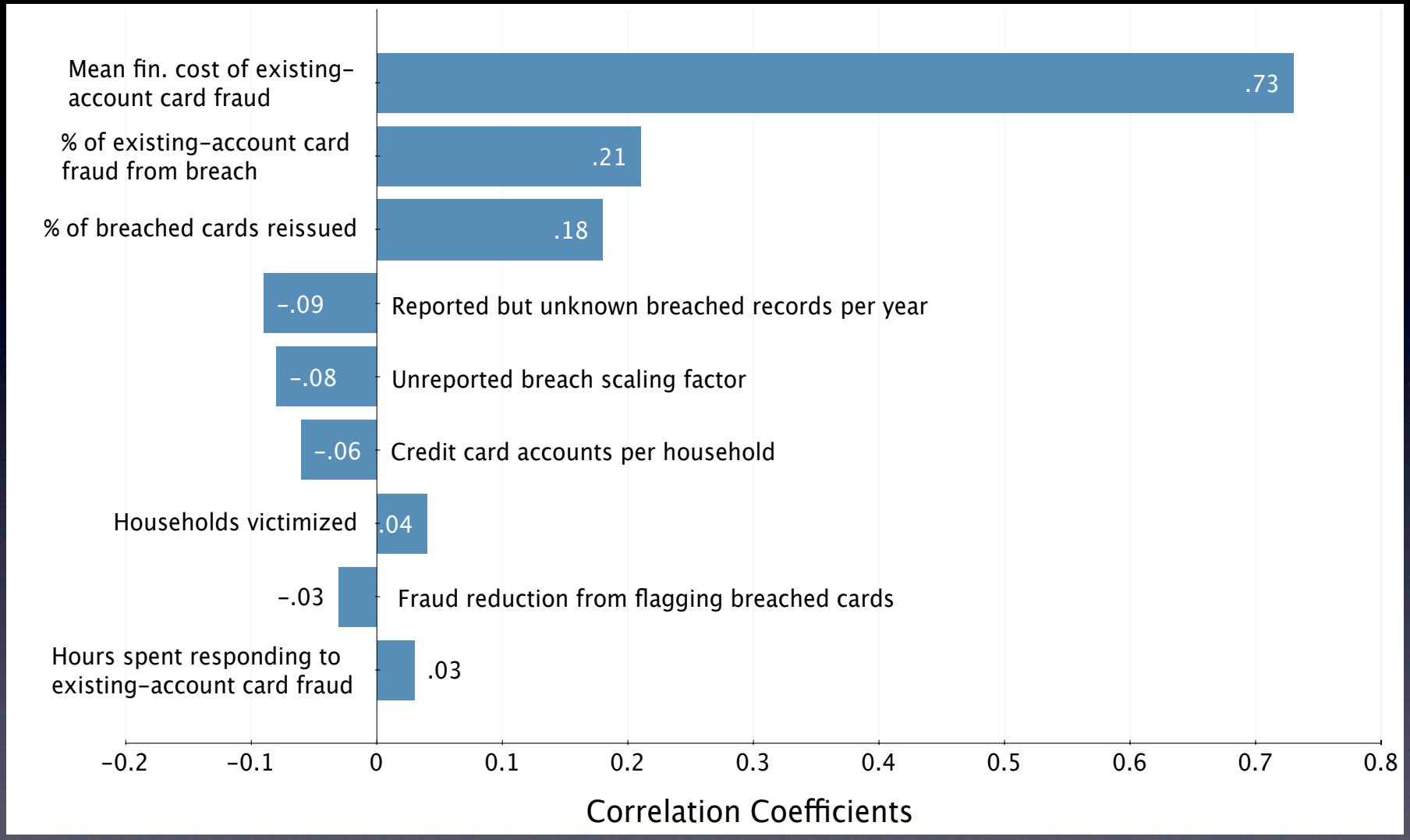
Monte Carlo Analysis of Results

Per-Card Costs



Total Cost Savings by Not Reissuing




Mean fin. cost of existing-account card fraud
.73
% of existing-account card fraud from breach
.21
% of breached cards reissued
.18
-.09
Reported but unknown breached records per year
-.08
Unreported breach scaling factor
-.06
Credit card accounts per household
Households victimized
.04
-.03
Fraud reduction from flagging breached cards
Hours spent responding to existing-account card fraud
.03
-0.2
-0.1
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
Correlation Coefficients

Where to Improve Data?

Data	How to Address it?
Percent of fraud resulting from breach	More study
Effectiveness of fraud monitoring	Issuer disclosure?
Number of undetected and undisclosed breaches	Incentives to detect and disclose?

Conclusions

- Reissuing cards immediately after a breach may be *more* expensive than waiting until fraud is attempted.
- But this depends greatly on data that needs improvement.

Questions?