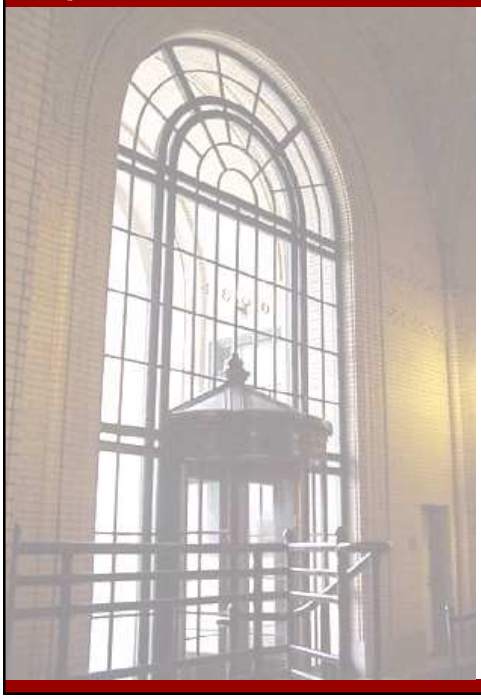
Carnegie Mellon



Do data breach disclosure laws reduce identity theft?

Sasha Romanosky

January 8, 2008

ISSA™ Information Systems Security Association
The Global Voice of the Information Security Profession

Carnegie Mellon Information Security Policy & Management | Heinz School

Carnegie Mellon

A familiar public policy question:

What is the effect of X on Y?

For example, what is the effect of:

- Abortion on crime (Levitt and Donahue, 2001)
- Minimum wage increases on employment (Card and Krueger, 1994)
- Concealed guns on violent crime (Rubin and Dezhbakhsh, 2003)

Carnegie Mellon Information Security Policy & Management | Heinz School

The problem: Identity theft

- FTC recorded over 250,000 idtheft consumer complaints (2005)
- Actual number of victims estimated to be between 8.3 - 8.9M
- Total amount stolen is estimated at over $56B (Javelin, 2006)
- Impacts include costs to
  - Consumers: time repairing credit damage, lawyer fees, etc
  - Firms: loss of reputation, law suits, fines, call centers. E.g. costs to Choicepoint: $15M, TJ MAX: $118M

The Cause?: Data breaches

- Are they really that prevalent? (SANS NewsBites 12/01/07)
  - Cyber Intruders Access National Lab Visitor Database (2 days ago)
  - Stolen Laptop Holds Forrester Employee Data (3 days ago)
  - Twin Cities Blood Donor Data on Stolen Laptop (3 days ago)
  - Canadian Passport Site Data Leak (last week)
  - Laptop Stolen From Auditor's Car (last week)
  - …
- (It would seem so..)

The solution?: Data breach disclosure laws

- These disclosure laws require firms to notify consumers when their personal information has been lost or stolen
- Many people feel these laws will reduce IDTheft
  - US Congressional hearings (US 2005, 2006)
  - "among the most important advances that the [UK] could make in promoting personal internet security" [Science and Tech Committee, 2007)
- Significant precedent of US disclosure laws: EPCRA, FDA, Hazardous Substances Act, Nutrition labeling, Fuel Octane levels

But why should they work?

Sunlight as a disinfectant

- Shining a light on a firm's poor security practices will encourage them to improve (reducing the externality)
- "Drive performance through transparency and public oversight" (Mulligan 2007)

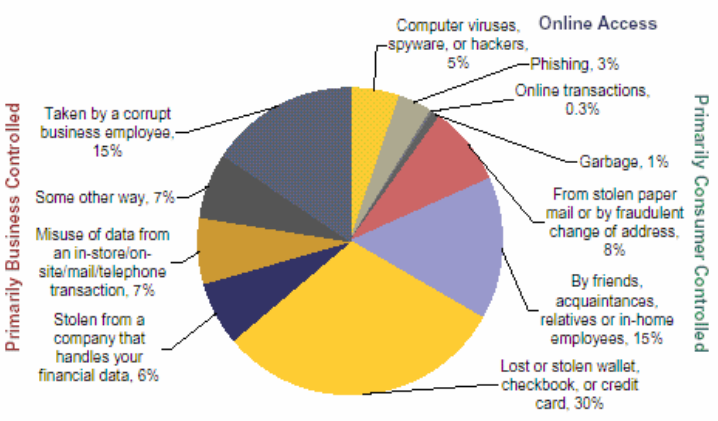
Right to know

- Consumers have the right to know when a firm is using, or abusing their information.
- By notifying consumers of breaches, they can mitigate the risk (close accounts, warn banks/CC firms, freeze credit)

Not everyone agrees…

- Laws cause firms and consumers to incur unnecessary costs, leading to an overall worse outcome, if the actual likelihood of idtheft conditional on a breach is as low as 1% (idAnalytics, 2006)
- The externality is not nearly so grave: firms already bear ~90% of the cost of breaches (Javelin Research, 2003, 2005, 2006)
- Consumers could become desensitized to numerous breach notifications, ignoring all of them
- Stifles ecommerce and R&D by discouraging firms to innovate (Rubin and Lenard, 2005)

Sources of Identity Theft



For those victims who knew source, 35% reported it was due to data breach. (Javelin Research, 2006)

Data breaches

Business Type	Count	Percentage	Total Records Lost	Avg No. of Records Lost
Business	234	33%	153M	650K
Educational	225	32%	5.7M	25K
Government	176	25%	42.7M	240K
Medical	70	10%	4.5M	65K
Total	705	100%	206M	290K

~ 70% of breaches cause by hackers (stolen data)
~ 25% caused by employees (lost data)
~ 75% of breaches include SSN

Source: Attrition.org, 2002-2007

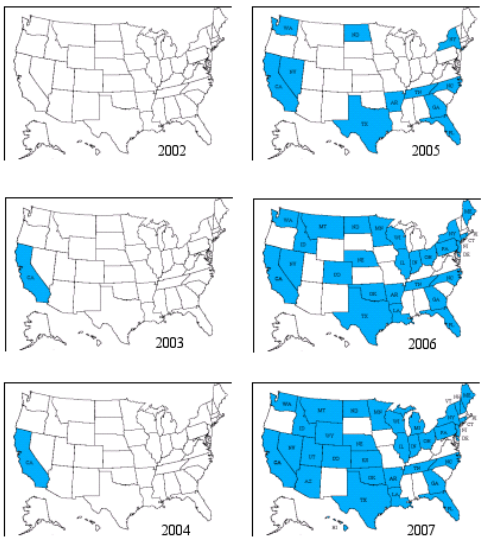
The first data breach law

- California adopted the first law in 2003, SB 1386
- Partially modeled after the EPCRA in an attempt to inform consumers and improve firm practices.
- SB 1386 has been the model by which most other states crafted their laws

Characteristics of the laws

- **Definition of a breach**: "unauthorized acquisition of data that compromises CIA of PII…"
- **PII**: first and last name in addition to some other kind of identifier (medical, biometric)
- **Trigger**: acquisition-based and lower threshold vs. risk-based and higher threshold
- **Covered entities**: state agencies, data brokers, private businesses. GA applies to just data brokers (why?)
- **Exemption**: exception for GLBA, HIPAA, if law enforcement is involved, if data is encrypted, or if data is already public

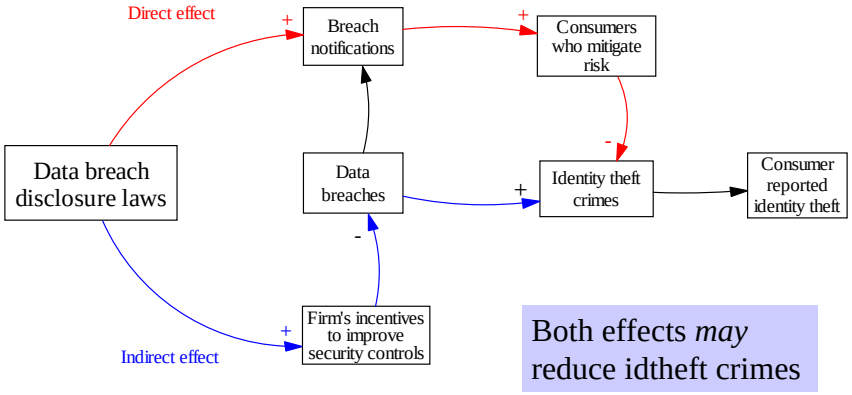
- **Important**: it is the residency of consumer that dictates disclosure, not the location of the breach



Adoption of state laws, 2002 - 2007

Year	# adopters
2002	0
2003	1 (+1)
2004	1 (+0)
2005	11 (+10)
2006	28 (+17)
2007	38 (+10)

Causal Data Model



Identity theft Data

- The FTC maintains a national database on consumer-reported identity theft complaints
- Monthly data from 2002-2006, acquired from FTC with FOIA request, aggregated to semi-annual periods (smallest period over which we expect to see an effect of law)
- 5 years * 51 states (including D.C.) = 510 obs

Econometrics

- Using statistics to help answer a public policy question
- Provides evidence to support (or refute) a causal relationship. (i.e. do data breach laws reduce identity theft?)

- Need to control for other, potentially important variables, that could also influence levels of identity theft.
- For instance, state and time effects, presence of credit freeze laws, unemployment levels, FACTA, state demographics, etc.

Preliminary results

- Overall, we find no significant effect of law on identity theft, even after 18 months

But does the law affect all states equally?

- We find that for higher income states, law appears to reduce identity theft by 3% by adoption, and raises to 7.3% after 18 months of adoption
- Unexpectedly, law seems to increase identity theft by 9.8% in lower income states

Future Work

- Is law adoption truly exogenous? (shock, lobbying, political skill)
- We'll test whether stricter laws have a stronger effect
- Where do we expect to see stronger effects of laws? Likely, where identity theft is most prevalent (BJS 2007) :
  - households in western states,
  - living in urban/suburban areas

Are these laws useful?

- What do you think?
- Should they be more or less strict?
- Should notification be more or less frequent?
- Should penalties be more or less harsh?
- Or do we just wait and see what happens?

Questions?

http://explodingdog.com/rocketguy.gif